The NIS Law

– A Milestone for Security Standards

Bachelor Thesis

International Management

Supervisor: Eva Aileen Jungwirth-Edelmann, MA

Author: Larissa Stella Reichl

1721025

Vienna, 17-05-2020

Affidavit

I hereby affirm that this Bachelor Thesis represents my own written work and that I have used no sources and aids other than those indicated. All passages quoted from publications or paraphrased from these sources are properly cited and attributed.

The thesis was not submitted in the same or in a substantially similar version, not even partially, to another examination board and was not published elsewhere.

17.5.2020

Date

Abstract

Topic: Impacts of the NIS law on Austrian operators of essential services

Name of Author: Larissa Stella Reichl

Course/ Year: BSc International Management / 2020

Pages: 87

Content: The European Commission established the Directive (EU) 2016/1148 of the European Parliament and of the Council, entailing measures for a high common level of security of network and information systems across the Union (NIS Directive 2016), which was carried out into national Austrian law in 2018 (NIS law). Since cyber-security and legal regulations are always a controversial topic, this law can either be seen as a milestone for security standards or as a burden for operators of essential services. The objective of this study was to investigate the economic and organizational impacts of the NIS law on Austrian operators of essential services.

The empirical research was conducted by qualitative content analysis of legislations, numerous publications of the EU and further literature. In the next step, the qualitative method of interviews was used, including on the one hand members of the authorities, on the other hand members of operators of essential services as well as an advocacy group.

The main findings of this research were that, while the elaboration of the NIS law was fulfilled as desired, the actual implementation remains questionable. There is a variety of benefits expected from this law, such as process optimisation and harmonisation, sensitisation and enhanced awareness of employees, better collaboration as well as uncomplicated and fast exchange of information in the event of threats affecting cyber-security. However, while the authorities are highly enthusiastic about the NIS law, its actual necessity is doubted by some operators of essential services, mostly due to the potential overregulation and overcomplication and therefore unjustifiable efforts demanded from enterprises.

Supervisor: Eva Aileen Jungwirth-Edelmann, MA

Table of Contents

List of Tables

List of Figures

List of Abbreviations

BSI: Bundesamt für Sicherheit in der Informationstechnik (Federal Agency for information technique)

CERT: Computer Emergency Response Team

CIRT: Computer Incident Response Team

CIA: Confidentiality, Integrity, Availability

CIP: Critical Infrastructure Protection

CIPS: Consequence Management of Terrorism and other Security-related Risks programme

CIS CSC: Centre for Internet Security

CSIRT: Computer Incident Response Team

ECI: European Critical Infrastructure

ENISA: European Network and Information Security Agency

EPCIP: European Programme for Critical Infrastructure Protection

EU: European Union

GDPR: General Data Protection Regulation

GovCERT: Government Computer Emergency Response Team

IKDOK: Innerer Kreis der Operativen Koordinierungsstruktur (Inner circle of operational coordination structure)

ISO: International Organization for Standardization

ISA/IEC: International Society of Automation/International Electrotechnical Commission

IT: Information Technology

KRITIS: Kritische Infrastrukturen (Critical infrastructures)

LFG: Luftfahrtgesetz (Aviation law)

NIS: Network and Information Security

NISG: NIS Gesetz (NIS law)

NISV: Netzwerk- und Informationssystemsicherheitsverordnung (decree on network and information system security)

SPoC: Single Point of Contact

1 Introduction

The internet is a vital ingredient to facilitate our everyday lives. The western world is strongly dependent on its proper and uninterrupted functioning, since most systems depend on it. In order to ensure the quality of modern human daily living, the provision of service systems, including health, energy and transport, is a necessity. According to Müller (2014), a consultant for security and project management, the internet is vulnerable to cyberattacks and therefore needs to be protected, in order to secure fundamental rights, security and privacy.

Hence, the European Union, along with its institutions such as the ENISA (European Agency for Network and Information Security), set itself the goal to address the protection of citizens with all the factors associated with it, as mentioned above. Critical infrastructures have become a highly coveted target not only for terrorist but also for cyber-attacks. In order to raise awareness and improve their protection, the EU has on the one hand allocated a large spectrum of resources in the format of many funding programs and on the other hand, established directives (European Commission, 2013b).

1.1 Motivation and Cognitive Interest

Our whole society is reliant on the constant provision of properly working systems, for example in healthcare, transportation and energy, which are highly dependent on frictionless operation of information systems, as well as on the constant availability of the World Wide Web. While the various benefits provided by the internet seem to be endless, it is not just a big opportunity but also a threat (Müller, 2014).

According to the *European Commission* (2013), the protection of fundamental rights, freedom of speech, personal data and privacy are essential for cybersecurity's effectiveness, as enshrined in the *Charter of Fundamental Rights* and core values of the EU. Hence, safeguarding individuals without safe networks and systems is impossible. Any information sharing of personal data, aiming at cyber-security ought to value and protect the individual's rights and be compliant with EU data protection law (European Commission 2013).

Cybersecurity, also known as *information security or electronic information security*, can be defined as the practice of defending all devices connected to the internet, i.e. servers, computers, mobile devices, networks, electronic systems and data from malevolent attacks (Kaspersky, 2017). The term cybersecurity is to be found in a variety of contexts and can be split into common categories: network, application, information, operational, and disaster recovery and business continuity (Kaspersky, 2017).

Cybersecurity has become a major concern for today's society and is therefore an important issue, which has to be addressed by policy makers across borders. Hence, the European Commission was impelled to establish the Directive (EU) 2016/1148 of the European Parliament and of the Council on 6 July 2016, entailing measures for a high common level of security of network and information systems across the Union (NIS Directive 2016) on August 8th 2016. After more than two years, the directive was incorporated into national Austrian law - *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen* (NISG, 2018).

1.2 Outline of the Thesis: Research Questions, and Hypothesis

Due to the reasons given above, this research will investigate how companies will react to such a law. Usually, either enterprises apply internal, grown security standards or resort to existing standards. However, the decision on which standards should be applied and on how security management should be properly implemented is still up to the operators of essential services. Nevertheless, companies are now faced with a controversial situation, where not only minimum-security standards are dictated by law, but also severe incidents have to be reported.

Consequently, this leads to the main aim of this thesis, which is to analyse the organisational and economic impacts on operators of essential services caused by the NIS law.

In order to analyse this topic, the researcher needs to start with the research of the primary source, which is legislation, namely the NIS Directive and Austrian NIS law. As

a second step, minimum-security standards need to be examined, to receive a clear picture in order to be able to design questions supporting the goals of this research.

Hence, the following research questions were identified as secondary aims:

Law

- What does the NIS law state?
- Which obligations are set by the NIS law?
- What were the reasons for the non-application of existing standards in Austria, such as ISO 27001 and BSI Grundschutz, and which major adaptions has the NIS law experienced?
- Is there any intention to create sector specific standards[1], such as for water, health and infrastructure?
- Does the NIS law fulfil the EU goals concerning cybersecurity?
- Does the NIS law conflict with the GDPR (General Data Protection Regulation)?

Organisations

- Can the cooperation between companies and the state be improved? Can companies' performance be enhanced?
- Does the NIS law induce changes within organisations?
- What kind of organisations are affected by the NIS law?
- Is management commitment apparent?
- Does the personal have all competences necessary in order to implement all obligations set by the NIS law properly? Does additional workforce (from outside) need to be hired? Does this lead to security issues?
- Are the organisations' budgets sufficient or are additional resources required?

Compliance

- What measures need to be taken in order to be compliant with the NIS law?
- Do authorities provide support to organisations?
- How and by whom is Austria's adherence to the NIS law monitored?

[1] Already many security standards exist, but they are specific to each sector, with the directive a base standard shall be reached (ENISA, 2017).

- Does the NIS law cause any positive/ negative effects?
- What happens in case of non-compliance of operators of essential services, such as non-fulfilment of minimum-security standards or omission of incident reporting?
- Will sanctions or monitoring and subsequentially sanctioning occur frequently?
- Are the obligations set by the NIS law, such as the fulfilment of minimum-security standards, taken seriously by operators of essential services?
- Can overall transparency be enhanced by the obligation to report incidents?

Consequently, this leads to the main research question: What are the economic and/or organizational impacts of the NIS law on Austrian operators of essential services?

From the above, the following hypothesis results:

In spite of every effort, it will be practically impossible for operators of essential services to fulfil all requirements set by the NIS law.

1.3 Limitations of Study

The first limiting factor for the research is a restriction of time, since this thesis is due May 2020. In order to overcome this issue, extensive literature will be provided, as well as the analysis of the transposition of the NIS Directive and the comparison to other EU-Directives.

Furthermore, due to the fact that the NIS law has just been introduced, there is limited data available to analyse.

Nonetheless, the primary research will be based on the review of already existing literature. In order to overcome the lack of existing studies, the researcher will conduct expert interviews with participants who were involved in the law-making

process, as well as with security experts who are employees of operators of essential services.

Proper predictions about the success of the transposition of the NIS Directive are not possible, since member states are still within the implementation process. Thus, the likelihood of successful transposition may be estimated by analysing how EU member states abide by other directives.

Member states show different degrees of difficulty regarding the successful transposition of EU directives due to divergences in their national laws (European Commission, 2018c). Thus, national laws must be adapted, which might take some time and entail some infringement procedures by the European Commission. The number of infringement cases amounted to 419 new cases in 2018. Although this number seems to be rather high, the number of new transposition cases has denoted a decrease by 25 percent compared to the year 2017 (European Commission, 2018c). The table below shows the overall statistic of directives:

	New Directives	**Changes in existing Directives**
2019	44	26
2018	21	28
2017	19	33
2016	21	30
2015	16	26

Table 1: Statistics changes in existing directives

Europa EURLex, 2019

2 Literature Review

In order to support the main aim of this thesis, the investigation of companies' reactions on the NIS law, expert literature has been reviewed and will be provided in the following sections.

Firstly, it will be illustrated how European law works, with special attention on how and why the NIS Directive was implemented. The establishment of directives is displayed in the graph below.

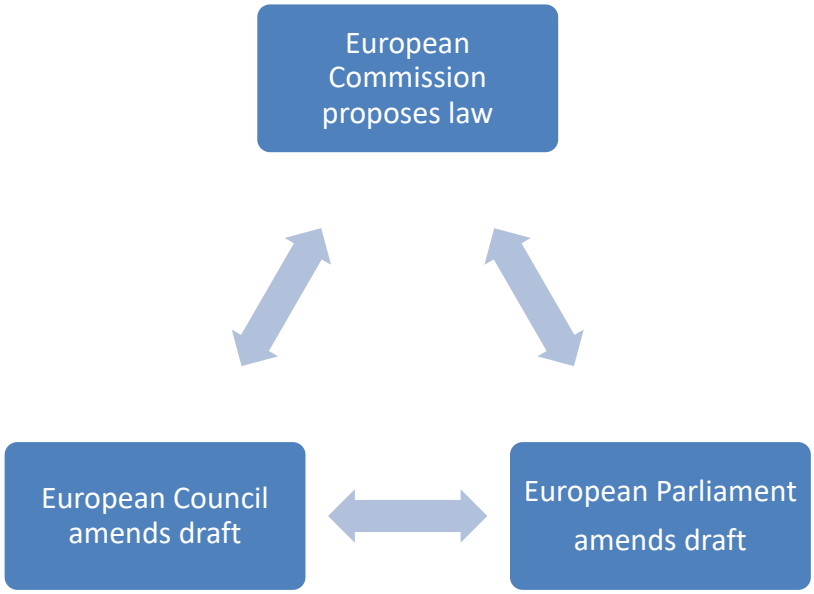


Figure 1: European Law

European Union, 2019, adapted by researcher

Secondly, the transposition of directives into national law will be explained.

If the directive is adopted by the Council and the parliament national governments have to implement the EU law.

Finally, security standards and incident reporting are the objects of this study, in order to understand the requirements and consequences of the law investigated, the NIS law.

2.1 The European Union and its Legislation Process

The European Union (EU), an economic and political union, consists of 27 member countries who are subject to all privileges and obligations of their membership and was founded in 1951. Austria entered the EU on January 1st 1995 and is currently holding 19 seats in the European Parliament (Europäische Union, 2019). Being a member state of the EU implies being part of the Union's founding treaties and subject to binding laws within the judicial and legislative institutions. The adoption of EU policies concerning foreign affairs is only possible if all member countries agree consensually (SchengenVisaInfo, defense 2019).

In the European Union, there are two main possibilities to establish law, either a regulation or a directive. While a regulation is a binding law that must be applied immediately by the member states, a *directive* is a legislative act, which defines a goal to be achieved by all EU countries (European Union, 2019). Nevertheless, strategies on the further elaboration towards these goals, respecting their national laws, are up to the individual member states. Each member country is obliged to incorporate directives set by the EU into its national legislation (European Union, 2019).

The proper application of EU law by member states is monitored by the European Commission (European Commission, 2019). Thus, the Commission is also dubbed the "guardian of treaties". In case of noncompliance, the Commission has to react and to take action if an EU state has not completely incorporated a directive into national law by the deadline set or might have applied the law in an incorrect manner. The determination of possible contraventions can be done by the Commission's own investigating efforts or by receiving of complaints of citizens, businesses, and stakeholders. Formal infringement proceedings can be instigated by the European Commission in case an EU country has not reported the measures for the complete implementation or does not remedy an alleged infringement against European law. The proceeding is divided into several steps, which are predefined in the EU contracts, each concluded with a formal decree (European Commission, 2019). As a first step, the regarded state receives a call letter from the Commission, requesting more detailed information that has to be communicated in an extensive written reply before the set deadline. If the Commission concludes that violation of provision according to EU law was committed, it sends an answer providing reasons, i.e. a

formal incitement, requesting the respecting country to act according to EU law and providing explanations why it is of the opinion that the country has violated the law. Furthermore, the member state is obliged to inform the Commission about the measures taken within the common deadline of two months. If the member country still does not correspond to EU law, the Commission may task the court of law with the case, which can then impose sanctions (European Commission, 2019). Measures, according to the court's judgement, must be performed by the member state. In case of discordancy with the judgement, the court may again be tasked by the Commission (European Commission, 2019). De novo, financial sanctions are inflicted. The amount of the fine is dependent on:

- the significance of the breached regulations
- whether well-being or personal interests are curtailed by the contempt
- for how long deployment of the respecting provision has been failed
- the country's financial resources

(European Commission,2019)

In this event, the penalty is meant to cause a deterring impact (European Commission, 2019).

As, according to the *European Commission* (2013), cybersecurity is and will be one of the most essential topics and especially critical infrastructure is the target of attacks, the next chapter will examine the background and the reasons that led to the implementation of the NIS-Directive (2016).

2.2 The European Union as a Protector of Critical Infrastructure

Any harm done to critical infrastructure, be it natural disasters or criminal or malicious activity, has significant impacts on the security of a state and the inhabitants. According to the *European Commission* (European Commission 2013a), critical infrastructure is either a system or an asset, which is substantial for a society's proper functioning. Any **failure or malfunctioning of these essential systems would cause sustainable shortfalls in supply, major disturbances of the public safety or other drastic consequences** (BSI – Kritische Infrastrukturen), 2019).

According to KRITIS (2017), the sectors of critical infrastructure are:

- **Government and administration:** existence of judicial organisations or the provision of emergency services
- **Energy** (e.g. electricity and gas supply)
- **Health** (e.g. medical care and provision of pharmaceuticals)
- **Information technology and telecommunication** (e.g. provision of telephone, telefax and internet)
- **Transport and traffic** (e.g. rail and road transport)
- **Media and culture** (e.g. provision of press, radio and television)

Source: KRITIS, 2017

The European Union has four main aims, which will be further elucidated in the section below.

- **Establishment of European citizenship** which implies the protection of fundamental rights and freedom
- **Securement of security, freedom and justice**
- **Promotion of social and economic progress, which** includes environmental protection, social and regional development, the Euro and the single market.
- **Assertion of Europe's role in the world**

Citizens Information, 2019

Addressing the first aim, stated to be one of the European Union's major objectives is the reduction of vulnerabilities of critical infrastructure and an increase in resilience (European Commission 2013a). Thus, adequate levels of protection must be ensured in order to minimize any detriment of disruption on societal needs. The framework for operations aiming to improve the protection of critical infrastructure across all states of the EU was set by the European Programme for Critical Infrastructure Protection (EPCIP) and other Security-related programmes (European Commission 2013a). This programme aims to include proper response to any kind of terrorism, criminal activity, natural disasters and various other causes for incidents. The EPCIP's

cross-sectoral approach is supported by regular exchange of information between EU countries during *CIP Contact Point meetings* (European Commission 2013a).

The program's major objective is the support for CIP policy priorities by provision of expert knowledge and a scientific fundament for enhanced comprehension of interdependencies and criticalities at all levels (European Commission 2013a).

A key point of this programme is the *Directive on European Critical Infrastructures,* enabling a procedure to identify and designate *European Critical Infrastructure* (ECI) (European Commission 2013a). This approach is stated to be common for the assessment of potentially increased need of protection. This directive is of sectoral scope and is applied to energy and transport sectors only. Furthermore, this directive requires owners or operators of assigned ECI to prepare Operator Security Plans and to nominate Security Liaison Officers, linking the operator or owner to the national authorities in charge for the protection of critical infrastructure. Under the *Prevention, Preparedness and Consequence Management of Terrorism* and other *Security-related Risks programme*, more than 100 projects were funded by the Commission between 2007 and 2012 (European Commission 2013a). The programme is destined for the protection of citizens and critical infrastructure from all kinds of security attacks, e.g. terrorist attacks, by supporting the improvement of protection of critical infrastructures as well as addressing crisis management (European Commission 2013a).

Our society is strongly dependent on a well-functioning infrastructure. However, maintenance of these vital functions is crucial for today's society, which forces security operators of essential services to undertake ongoing investments into their security (European Commission, 2018a). Nevertheless, the insurance of security and cybersecurity is not only a major challenge for companies but also for the state, for the economy and the society, not only in a national as well as in a cross-border context (European Commission, 2018a).

Cybersecurity is granted more attention than ever before, among policymakers, the industry, academics, and also among the public. Since adversaries have become more determined, sophisticated and more likely to be connected to a nation state, cyberattacks have also occurred more frequently, sophisticated and threatening.

Hence, growing insecurity concerning the privacy of data has grown. (Kuner et al. 2017).

As mentioned in the previous chapter, **measures to strengthen Cybersecurity by the NIS Directive provided by the European Commission** are as follows:

- Introducing national NIS Authorities and Incident Response Teams (CSIRTS)
- Encouraging strategic cooperation by setting up a Cooperation Group
- Notification of serious incidents
- Introducing minimum-security standards as well for operators of essential services as for digital service providers

European Commission, 2018a

Since companies are now forced to fulfil these minimum-security standards and are audited once every three years, the NIS law is a subject, which is either about to cause increased effort, monetary expenses or support for companies in their attempt to strengthen Cybersecurity (Asllani, Ettkin & White, 2013). Nevertheless, such a law will permanently be highly controversial because there will always be a gap between personal rights, patents and copyright on one hand and the fight against cybercrime on the other hand. According to Asllani, Ettkin & White (2013, p.12) “cybersecurity should be considered a public good provided by the government.”

2.3 EU Cyber Strategy leading to the NIS-Directive

According to the widely represented opinion that people who do not have access to the internet are disadvantaged living in our ever more digitalised world, each and everybody should be given access to the internet and its unhindered flow of information, while safe access must be guaranteed constantly (Helisch & Pokoyski, 2009).

However, the digital world is not under the control of a single entity, but under the control of various stakeholders, including commercial and non-governmental ones, who are part of the daily management of internet resources, standards, protocols and its future development (Helisch & Pokoyski, 2009). All of these stakeholders are

attributed high importance in the governance model of the internet by the European Union, which is why the EU also supports this multi-stakeholder governance strategy. Within all sections of human life, the growing reliance on information and communication technologies has led to the revealing of weak spots, which need to be defined, analysed, reduced or remedied in a sophisticated manner (Helisch & Pokoyski, 2009). Furthermore, Helisch and Polinsky state that all actors of relevance, i.e. individual citizens, the private sector and public authorities, need to register this shared responsibility in order to take measures towards self-protection and ensure coordinated response to strengthen cybersecurity if necessary.

Security starts with the human, since he is responsible to decide what kind of information needs to be secured in the best possible way (Helisch & Pokoyski, 2009). Hence, the human is security's most important component and therefore, its key factor. Accordingly, the human also becomes the greatest asset that can be used by companies to defend their information and communication systems and secure their processes. However, the human is also stated to be the biggest threat to the world of internet technologies, which can be well felt by the ever-increasing numbers of cyberattacks (Helisch & Pokoyski, 2009). In addition, the human's susceptibility to errors can never be fully inhibited.

Thus, security awareness is the crucial factor for the protection of not only organisation's but also human values. According to the infamous ex-hacker *Kevin Mitnick*, "Human Firewalls are a must!" (as cited in Helisch & Pokoyski, 2009, p5). This implies that information security needs to take place in people´s consciousness, not in technology.

Thus, the EU is required to safeguard the online environment while offering the highest freedom and security to the advantage of everyone (European Commission, 2013). By this strategy, proposing certain actions the EU's overall performance can be enhanced. However, the handling of cybersecurity challenges is still a predominant task of the member states. Both long and short term, these actions include a wide spectrum of policy tools and integrate several actors, i.e. the EU's institutions, member states or industry. In this strategy, the EU's vision presented is enunciated in five strategic priorities, which address the challenges described above (European Commission, 2013).

The priorities to be named are:

- The achievement of cyber resilience
- The drastic reduction of cybercrime
- The development of a cyber-defence policy and capabilities associated with the Common Security and Defence Policy (CSDP)
- The adoption of technological and industrial resources for the security of the cyberspace
- The establishment of a standardised international cyberspace policy for the EU and promotion of its core values

European Commission, 2013

Hence, cybersecurity has become a major challenge within the last years, since our daily life, social interactions, fundamental rights and economies are dependent on information and communication technology working coherently (European Commission, 2013).

The European Union is highly aware of these facts and has resultantly placed significant importance on the development and implementation of strategies in order to handle such incidents properly, including the securement of network and information systems in order to ensure prosperity as well as to keep the online economy safe. Accordingly, "Europe's strength lies in its diversity, skills and commitment to strong cybersecurity" (Bundeskanzleramt, 2014, p.1). Cyber-security is at the very top of EU priorities but also requires high-level expertise. Several measures regarding the securement of the European Digital Single Market and the protection of infrastructure, businesses, governments, and citizens have already been implemented by the European Union (European Commission, 2019a).

In terms of cyber diplomacy, more and more communication platforms are being used – some of them very secure, some of them insecure. Still "The European Union and its Member States strongly promote an open, free, stable and secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply for the social well-being, economic growth, prosperity and integrity of free and democratic

societies." (building strong cybersecurity in the EU (European Commission, 2019a, p.9). Furthermore, the European Union and its member states believe in the adoption of international law across all borders of the member states, compliance to rules and norms of responsible state behaviour and taking steps towards the establishment of confidence. In addition, the meaningfulness of outreaching capacity building and enhancement of global cyber resilience is expressed in order to beware conflicts and enhance cyber stability via the application of law enforcement, economic, legal and diplomatic instruments, such as sanctions (European Commission, 2019a).

2.4 Development and implementation of the NIS Directive in the EU

Due to all the concerns about cybersecurity, the European Commission was commissioned to establish the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive 2016) on August 8 2016.

On the 7th of February 2013, a process, under the responsibility of Commissioner Neelie Kroes of the European commission, with the procedure number 2013/0027/COD was initiated, working towards the achievement of a high common level of security of network and information systems across the European Union (European Commission, 2013b). The result and preliminary conclusion of this process at EU-level was the commencement of the NIS Directive on the 8th. of August 2016, under the legislative basis of article 114 of the *Treaty on the Functioning of the European Union,* which primarily addresses the proper functioning of the European Single Market (NIS Directive, 2016, Art 114 Paragraph 1).

The Directive on security of network and information systems (NIS) is the first part of a legislation on cybersecurity, the *EU Cybersecurity strategy*, within the European Union and was introduced to ensure the provision of legal measures to strengthen the level of cybersecurity across the EU (European Union, 2013). The primary aim of this directive is the **ascertainment of high common standards of network and information security** in order to enhance the internal market's functioning.

The NIS Directive is claimed to be the milestone of the EU's cybersecurity architecture because of its provision of legal measures to strengthen the overall level of cybersecurity and disposition of the European Union; a culture of security that covers the vital sectors of our economy and society is formed (ENISA, 2019). The sectors involved namely are energy, transport, water, banking, health care, financial market infrastructures, and digital infrastructure.

Furthermore, the directive was adopted in order to boost national cybersecurity capabilities by demanding member states of the EU to provide an enhanced cybersecurity strategy, a *Computer Security Incident Response Team* (CSIRT), NIS competent authorities and a single point of contact, all on a national level. The NIS Directive improves cooperation across member states of the European Union by the establishment of the CSIRTs Network, comprised of:

- EU member states' elected CSIRTs
- CERT-EU (Computer Incidents Response Team for the EU Institutions, bodies and agencies),
- the NIS-Cooperation Group,
- the European Commission and the EU Agency for Cybersecurity (ENISA).

ENISA, 2019

Furthermore, the establishment of a *computer incident response team network* (CIRTS network) was induced by the NIS Directive in order to be conducive to the development of trust and confidence between member states and support fast and effective operational cooperation (NIS Directive 2016, Article 9). The *Computer Emergency Response Team* (CERT) for the institutions, agencies and bodies of the EU is comprised of IT security experts being responsible for the major EU institutions (EASA, 2017).

These institutions are namely:

- European Parliament
- European Council
- Council of the European Union
- European Commission

- Court of Justice of the European Union
- European Central Bank
- European Court of Auditors
- European External Action Service
- European Economic and Social Committee
- European Committee of the Regions
- European Investment Bank
- European Ombudsman
- European Data Protection Supervisor

(European Union, 2018)

The CERT-EU is concerned with the cooperation with specialised IT security companies and other CERTS in the member states to ascertain the notification of cybersecurity incidents and cyber threats (EASA, 2017).

The *NIS cooperation group* forms a strategic cooperation group, where

- cooperation,
- exchange of information and
- compliance

on the development of strategies on how to implement the NIS Directive coherently across the EU within member states of the European Union take place (ENISA, 2019). Moreover, the group provides strategic direction to the underlying EU CSIRT (Cybersecurity Incident Response Team) network. The members of the group are representatives of relevant national cybersecurity agencies and national ministries.

Figure 2: EASA,2017; adapted by researcher

Such working documents were published by the *NIS Cooperation Group*, including guidelines concerning the implantation of the NIS-Directive (European Commission, 2019b). Moreover, these documents are stated to be the first part of an EU-wide legislation regarding cybersecurity and documents which address broader cybersecurity issues. Documents play a big role in the provision of assistance in the implementation of the NIS Directive concerning the identification of companies, operators of essential services, who are subject to the Directive´s demands and therefore the notification of serious incidents to member states of the EU. On top of that, the NIS cooperation group has prepared documents concerning the protection of elections and, even more important for Austria, a taxonomy. This taxonomy provides instructions on how to identify and categorize cyber incidents for common understanding. (European Commission, 2019b).

Additional working documents, published in February 2018, mainly addressed security measures and incident notification for *Operators of Essential Services* (European Commission, 2019b). The latest document published by the NIS Cooperation Group, labelled *"Guidelines on cross-border dependencies",* intends to support EU-member states with the collection of information and to trace their interdependencies risks related to the dependencies, that are likely to be able to assist them with the application of the proper measures mitigating risk on a national level (European Commission, 2019b). All these documents being part of the first biennial Work Programme (2018-2020) were introduced and adopted in February 2018 (European Commission, 2019b).

The primary goals were the deployment of deliverables by collecting all kinds of appreciable experiences in the area of cybersecurity as well as the contribution of all working Group members to identify best practices and guidance (European Commission, 2019b). Hence, the endorsement of deliverables was possible in July 2018 with regards to this cooperation and its constructive dialogue. The *NIS Cooperation Group* itself was instituted by the NIS Directive and began to work in February 2017. It consists of the European Commission, the European Union Agency for Network and Information Security (ENISA), and of representatives of all EU member states' national cybersecurity authorities. Accordingly, the dialogue between all bodies accountable for cybersecurity within the European Union is facilitated. The NIS Cooperation Group also functions as the EU's forum in which commonly arising cybersecurity challenges are being discussed and coordination of potential cybersecurity policy actions takes place (European Commission, 2019b).

The NIS Directive itself consists of three parts (ENISA, 2019);

1. The first one addresses the national capabilities and states that **member states of the European Union are obliged to have certain national cybersecurity capabilities** e.g. that they need to have a national CSIRT (Computer Security Incident Response Team) or execute cyber exercises.
2. The second part is in respect to to cross-border collaboration between EU-member states, such as the existence of the **operational EU CSIRT network** and the **NIS cooperation group**.
3. The last section is about the **national supervision of critical sectors**, which entails the supervision of cybersecurity of critical market operators in the respective state. By way of example, this includes ex-ante supervision in critical sectors, i.e. energy, water supply, health systems, transportation services, and the finance sector and ex-post supervision for critical digital service providers, such as domain name systems and exchange points (ENISA, 2019).

This NIS Cooperation group is constantly supported by the ENISA (European Union Agency for Cybersecurity) in four ways:

1. **Identification of good practices** in the EU-member states respecting the **realisation of the NIS Directive**, i.e. the transposition into national law
2. **Simplification of the EU-wide cybersecurity incident responding process** via the installation of thresholds, templates and tools
3. **Approval on common approaches and procedures**
4. **Resolution of frequently arising cybersecurity issues**

ENISA, 2019

The obligations for all member states of the European Union to adopt a national policy on network and information security are set as defined by the NIS Directive (NIS Directive, 2016).

Working in compliance with the directive´s claims, member states of the EU need to **safeguard their essential state functions**, especially to protect national security. Actions, which need to be taken, are the protection of information member states adjudge to be contrary to the relevant interests of their security and the maintenance of law, particularly to accord permission for the investigation, detection and the prosecution of criminal attacks (NIS Directive, 2016).

Operators of essential services and digital services providers are required to either ensure their network security and information systems or to notify incidents by a sector-specific Union legal act (NIS Directive 2016, Article 5).

The **implementation progress** is shown as follows:

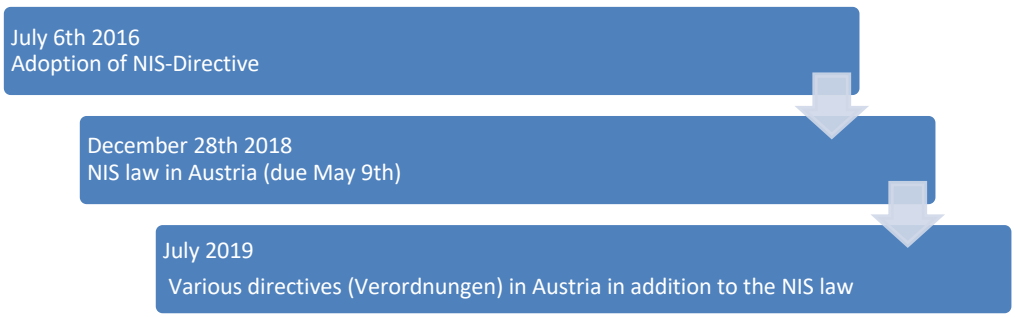


Figure 3: Implementation Progress

NISG, 2018; NISV,2019; adapted by researcher

The EU Directive on Network and Information Systems was adopted on the 6th of July 2016. Since then, member states were tasked to transpose and implement the NIS by adaptation of their current national legislation or by adoption of a new legislation (NIS Directive, 2016). In order to illustrate the wide-ranging requirements and obligations for Operators of Essential Services and Digital Service Providers, the NIS Directive national legislation tracker was introduced (ECS, 2019). This tracker maps out the national legislative member efforts and shows a brief outline of the national requirements for operators of essential services and digital service providers. Furthermore, relevant points of contact to facilitate the reporting or cyber incidents are highlighted (ECS, 2019).

2.5 Elaboration and Implementation of the NIS Law in Austria

First and foremost, the NIS law is meant to sub serve the **transposition of the NIS Directive into national law** (NIS Directive, 2016). The legislative operations for the implementation in Austria were performed by an interministerial working group consisting of representatives of the Federal Chancellery and the Federal Ministry of Interior and National Defence. The constitution and formulation of this draft law was, apart from the underlying directive set by the EU, dependent on a variety of other circumstances, which showed to have considerable influence on this draft. For everybody not being part of this working group, this process was entirely non-transparent (Bundeskanzleramt, 2019).

Built upon the fundamental alignment, the focus points of the NIS Directive were formulated. Due to this reason, there are strong variations regarding member states' levels of resilience and their approaches and strategies, which are stated to be undermining the security of network and information systems in the EU (NIS Directive, 2016, concerning measure 5). On top of that, strategic measures strengthening the cooperation between member states addressing the securement of network and information systems need to be supported and facilitated (NIS Directive, 2016, concerning measure 4). Hence, it can be stated that a comprehensive approach on EU-level entailing common minimum standards, cooperation, and mutual security

standards for operators of essential services and digital service providers is a necessity (NIS Directive, 2016, concerning measure 6).

The Austrian NIS law (Network and Information System Law), implemented on the 28th of December 2018, i.e. the NIS Directive was transposed into national law. Thereby, tasks resulting from the directive are to be assigned to already existing structures (Bundeskanzleramt, 2019).

The NIS law (2016) lays down tasks and obligations for the authorities responsible for the implementation and their capacities. According to NIS law, the Federal Chancellor is in charge of strategic operations, whereas operational tasks are in the responsibility of the Federal Minister of Interior. Within the material scope of application are e.g. ***operators of essential services*** of the sectors of **energy**, **air**, **transportation**, infrastructure of **financial markets, health care, water supply** and **digital infrastructure**, but also bodies of the **public administration** (Bundeskanzleramt, 2019).

The Federal Chancellor is primarily tasked with strategic operations (Bundeskanzleramt, 2019). Hence, it is within his duties to represent the republic in EU-wide and international committees of strategic tasks, as well as the implementation of a strategy to coordinate the public-private cooperation and the annual report of cybersecurity.

On top of that, the **determination of cybersecurity incidents** is also the Chancellor's responsibility (NISG, 2018, §4). Accordingly, he is the one to set further regulations for the respective sectors, for safety measures, for regulations regarding exceptions and regulations of duties of operators of essential services. The operational aspect of the Chancellor's work is the **securement and indemnity of Computer Emergency Response Teams** of the public administration. In addition, he is entitled to pass on data, pursued to paragraph 2-5, to foreign safety authorities and security organisations according to paragraph (NISG, 2018, § 2 Abs. 2 and 3) of federal law regarding international police cooperation (Polizeikooperationsgesetz – PolKG) BGBl. I Nr. 104/1997 and to deliver data to political entities of the European Union and the United Nations.

The Federal Minister of Interior is in charge of central operational tasks, e.g. the running of the central contact point (SPOC), the organisational administration of operational coordinating structures (IKDOK), the receiving and analysis of incident notifications, the examination of safety precautions, the adherence of incident response obligations and the assessment and review of qualified entities (NISG, 2018, §6). On top of that, the Federal Minister of Interior is responsible to enact more detailed regulations for the qualified entities.

Operators of essential services are public or private facilities settled in Austria, which provide an essential service in one of the sectors mentioned in the NIS law. This essential service must be controlled by information systems and is characterised by its significant importance regarding the maintenance of the public health sector, supply of public water, energy and vital goods, public transportation systems and the functional capability of public information and communication technology (NISG, 2018, § 17 Abs 1). According to the law, a service is of essential significance inasmuch as it is defined as an essential service in the NIS Directive. In the appraisal, whether a service is an essential one, was notably defined by its number of users, the subjection of other operators of this service, the geographical dispersal of a security incident, potential impacts of outages and the criticality of a service. On top of that, sector-specific factors were taken into consideration. According to the NIS law (2018, §16 and 17), it is of the Chancellery's responsibility to define the operators of essential services settled in Austria for each sector mentioned above.

When an institution is rendered an essential service, it receives a decree from the Federal Chancellor in which it is declared to be an essential service (NISG, 2018, § 16). If prerequisites cease to exist or it is ascertained that they had not been propounded beforehand, the institution is also notified by decree that it is not any more operator of an essential service. Within two weeks after the receipt, *operators* of essential services are obliged to name a contact point with the Chancellor, the Federal Minister of Interior or the computer emergency response teams (NISG, 2018, § 16).

Operators of essential services are obliged to fulfil a number of safety measures, possibly according to sector-specific standards, and to furnish proof at least every three years. Sanctions have to be paid in case provision of evidence was omitted,

denial of review/inspection by the Federal Ministry of Interior, belated execution of orders (NISG, 2018, § 26).

Furthermore*, operators of essential services* are committed to notify the responsible *CSIRT (Computer Incident Response Teams)* whenever security incidents occur (NISG, 2018, § 26). This notification is then instantaneously forwarded to the Ministry of Interior. Likewise, voluntary notifications to the authorities can be made. In case of omission of, fines up to 50.000 euros for single occurrence and up to 100.000 euros for repeated omission of provision of evidence have to be done.

The establishment of CSIRTs, or CERT (Computer Emergency Response Team), is stated to be a necessity to ensure the secureness of network and information systems (NISG, 2018, § 14, Abs. 1). To this end, the national computer emergency team and sector-specific computer emergency teams support *operators of essential services* and *digital service providers* as well as the *computer emergency team of the public administration (GovCERT)* and bodies of the public administration in the management of risks and security incidents. Tasks which are to be fulfilled by the *CIRTs* are the receiving and forwarding of concerning risks, incidents and security incidents to the Federal Minister of Interior, the output of warnings, alarms and recommendations, information spread about risks and incidents, technical assistance in case of a security incident, analysis of risks and incidents and status reports and participation in coordinating structures and the CSIRTs Network (NISG, 2018, § 14, Abs. 1).

Furthermore, sector specific CSIRTs can be installed by *operators of essential services* themselves, whereas *digital service providers* can task the national computer emergency team. **CSIRTs, being responsible for data protection law**, are authorised to process individual-related data, inasmuch as it is required for the achievement of the goals of the NIS law (2018, § 9 Abs. 2 bis 4).

The CERTs are obliged to satisfy the following requirements according to the NIS law (2018, § 14):

- **Standardised and installed in safe locations;** premises as well as the supporting network and information systems are standardised and installed in safe locations.

- **Securement of continuance of service;** especially by the application of a suitable network for the administration and forwarding of inquiries as well as by incessant availability of personal, technical and infrastructural equipment
- **Verification of support for operators of essential services;** personnel must be qualified, well instructed, and put through security clearance to access to secret information every five years
- **Use of secure communication channels,** which were decided on beforehand in consultation with the Federal Minister of Interior.

(ECS, 2019

The Federal Chancellor and the Federal Minister of Interior assess whether a CERT fulfils its duties (ECS, 2019). In case a CERT happens to be a private facility, it is to be authorized to fulfil all duties assigned and is furthermore obliged to communicate changes in circumstances that are requisite for the assessment of its eligibility. Authorization is repealed if conditions are no longer given (ECS, 2019).

In Austria, the transposition of the NIS Directive is still in progress (ECS, 2019). Most recently, the "*Verordnung des Bundesministers für EU, Kunst, Kultur und Medien zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssystemsicherheitsverordnung* – NISV)", which will be discussed in the next subchapter, came into effect on 17th July, 2019 (ECS, 2019).

2.6 Minimum-Security Standards

By the NIS law (NISG, 2016), *operators of essential services*, *digital service providers* and institutions of public administration are required to **fulfil certain *minimum-security standards.***

According to ICT and information technology security, norms and standards include processes, methods and proceedings. These standards consist of various modules, such as.:

- Baseline security
- Management systems
- General requirements
- Risk management

These standards are of significant importance for government authorities and operators of essential services and have been established widely in Europe (BSI, 2017).

2.6.1 Legal Basis

All operators of essential services must fulfil the minimum-security standards as defined in the *„Verordnung des Bundesministers für EU, Kunst, Kultur und Medien zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssystemsicherheitsverordnung – NISV", 2019).* This means that a number of **securement measures are audited and monitored** by the authorities responsible, namely the NIS authority. Audits are executed by the so called "*Qualifizierten Stellen*, companies which are accredited by the Ministry of Interior. Audit reports must be sent to the Ministry by the operators of essential services (NISV, 2019).

Each of these operators is assigned to the corresponding sector, namely the sectors:

- Energy
- Transport
- Banking
- Financial market structures
- Health
- Water supply
- Digital infrastructure

Netz- und Informationssystemsicherheitsverordnung – NISV", 2019

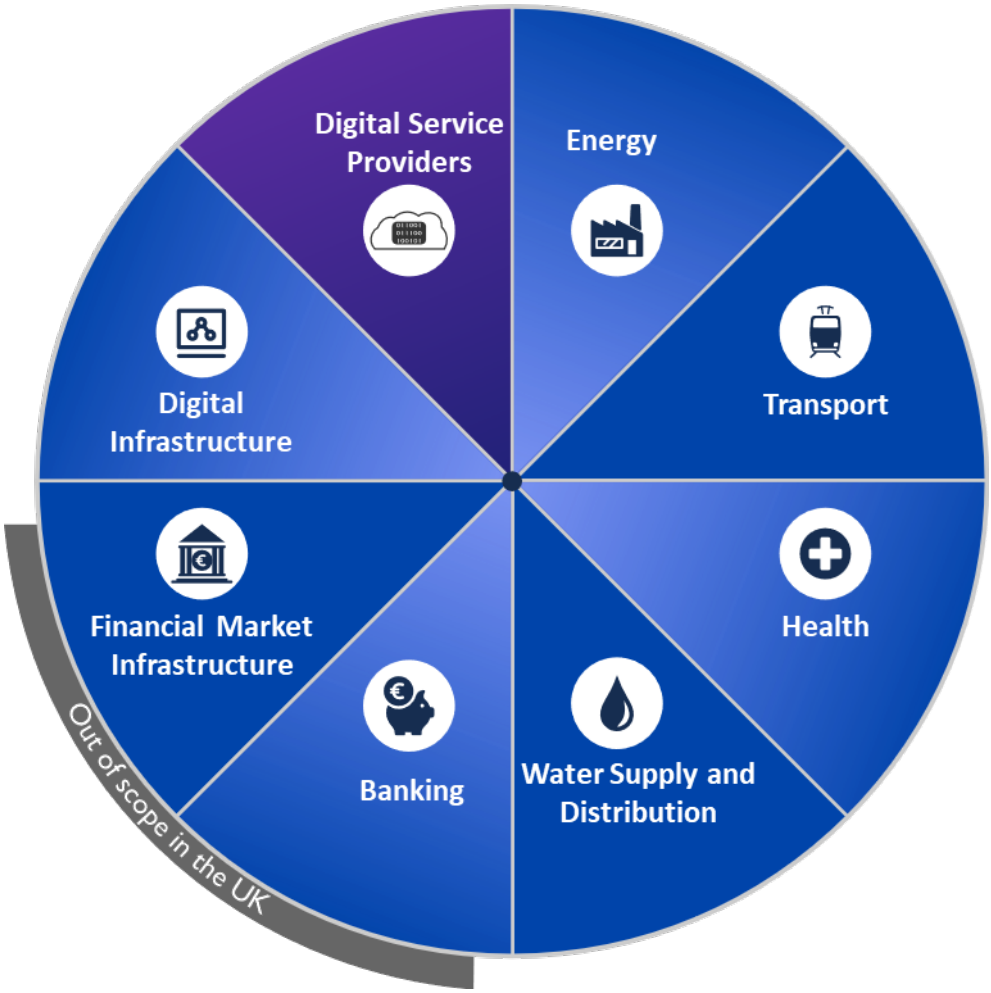


Figure 4: ENISA – Areas affected by the NIS Law

ENISA releases online NIS Directive Source: ENISA, 2018

The decree § 14 defining and categorising the security measures that have to be fulfilled entered into effect on the day of its announcement, July 17th, 2019.

These measures are:

Category	Measures
Governance und Risk management	Risk analysis
	Security policy
	Verification of network and information systems
	Resource management

	Information security management systems
	Human resources management
Supplier management	Supplier relationships
	Performance agreements
Security architecture	Configuration documentation
	Assets
	Network segmentation
	Network security
	Cryptography
System administration	Administrative rights
	Administrative systems
Identity and access management	Identification and authentification
	Authorization
System maintenance and operation	System maintenance and operation
	Remote access
Physical safety	Physical safety
Detection of incidents	Detection
	Protocolling and monitoring
	Correlation and analysis
Mastery of incidents	Incident response
	Incident report
	Incident analysis
Operating continuity	Operating continuity
	Emergency management
Crisis management	Crisis management

Table 2: Required measures for operators of essential services

NISV, 2019

By means of certain threshold values, operators of essential services are identified, as it will be elucidated by means of the Vienna International Airport (NISV, 2019). Within the subsector air transport, a facility, in this case of the sub-sector air traffic an airport, must fulfil the following requirements in order to be identified as an operator of an essential service:

- Commercial carriage by an aviation company, which carries more than 33 percent of yearly, checked in passengers at an airport, which denotes more than ten million yearly check ins.
- Flight handling, flight check-ins, luggage check-ins and operation of security systems.

NISV, 2019

Air traffic control, including the existence of air navigation services acting accordingly to the General Aviation law *(Luftfahrtgesetz (LFG), BGBl. Nr. 253/1957)* and the provision of aerodrome control services.

2.6.2 Definition of Organization, Values and Measures

An *organisation* is defined as every institution composed of humans and resources working together in a systematic manner in order to achieve certain strategic goals. It can be strictly structured, e.g. companies or government agencies, or an association without pursuit for profit (Vahs, 2009).

Information assets in the classical sense are usually confined to, pieces of information, data, computer files, and data storage devices (Kersten & Reuter, 2016). IT-systems and networks which process and transfer these information assets usually come in addition. For all these information assets, security objectives are to be defined. The generality usually pictures information as everything that is essential for the business operating ability, such as (Kersten & Reuter, 2016):

- Information concerning the company's operational capability, data, data sets, and registers
- Private documents such as contracts process instructions, emergency handbooks, and training documents
- External documents such as system descriptions and user handbooks
- All kinds of protocols and records
- Physical assets, i.e. technical components such as computers, firewalls, and gateways
- Infrastructures, i.e. server rooms, data centres, and all kinds of supply
- Software systems and development tools

- Services rendered or used by the organization itself, e.g. telecommunication services, data transmission, air conditioning, lightening, and electricity supply
- Qualified and experienced employees in assigned positions
- Further intangible assets such as the organisation's reputation or its creditworthiness

Kersten & Reuter, 2016

Since it is detectable that an organisation's assets are not only comprised of information, data and IT, but of the collectivity of infrastructural, organisational, personnel-wise, and technical components which an organization is characterized by (Kersten & Reuter, 2016).

Comprising there are three **base values for IT-security**:

1. **Integrity** aims at completeness and rightness, meaning any changes only can be done by authorized users.
2. **Availability (CIA)** denotes the feature of a value that an authorized user has access whenever needed.
3. **Confidentiality** ensures that information is only delivered to authorized subjects.

Kersten & Reuter, 2016

Having now characterized many security goals that ensure a safe and secure IT, it is necessary to define according security measures. Many of these measures are provided by the NISV (2019) and hence they have become mandatory tasks. In order to explain the *minimum-security standards* and the measures going along with them, the example of risk management is used.

2.6.3 Risk Analysis

The risk matrix is always a combination of probability of occurrence and consequences of an incident. In order to receive a matrix, it is vital to set the following steps:

- Risk identification: vulnerabilities must be identified especially those without countermeasures
- Risk assessment: the risk must be estimated and classified

- Risk score: the risk must be seen in the context to the organization, the importance for the organization has to be measured
- Risk treatment: starting with the highest classified risk proper measures are assigned to each risk

Kersten & Reuter, 2016

This is just one example out of 29 measures in the NISV (2019) that has become mandatory for operators of essential services and will be audited by qualified authorities (*qualifizierte Stellen).*

2.6.4 Audit

Operators of essential services are **legally obliged to have their services audited once every three years.** However, independent from law, conformity of an organisation to standards will show whether it is competent in IT security (NISV, 2019).

However, even if the findings of an audit should indicate the existence of deficits or deviations from the standard, the result of the audit must be rated positively. Room for improvement exists, which can be subject to the next working package (Kersten & Reuter, 2016). Referring to the NISV (2019), deficits will cause a decree with the request to eradicate the insufficiencies.

In the case of noncompliance, administrative penalty proceedings will be initiated:

- If no contact person is named
- If no audit report is delivered
- If the audit is denied
- If the via decree ordered actions are not fulfilled in time

(NISG, 2016, §26)

The penalty charge is 50.000euros, in case of recurrence 100.000euros (NISG, 2016, §26).

2.7 Incident Reporting

One of the main **reasons an *incident reporting system*** has entered into force is stated to be the **non-existence of such a regulatory system** in the whole European Union (Nagyfejeo, 2018). Telecom providers formed the only exception being the only

entities who already had to report their incidents before. Therefore, the NIS Directive was the ideal instrument to set up a strong regulation covering various cyber cultures (Nagyfejeo, 2018).

Since **cybersecurity incidents are unhindered by national borders** and as history shows, numerous incidents were indeed not limited to single countries, it is absolutely necessary for all member states to act on common principles (ENISA, 2018a).

Many **advantages** go along with **effective incident reporting**:

- Fast distribution of information to all participants
- Coordination of responses and potential inclusion of different members input
- Access to expertise over the whole EU, not limited to single nations
- Identification and enhancement of good and best practices and dissemination of impractical or useless methods

ENISA, 2018a

One of the key policy documents is a "*Good practice guide on incident reporting*" created by ENISA.

The main goals mentioned are:

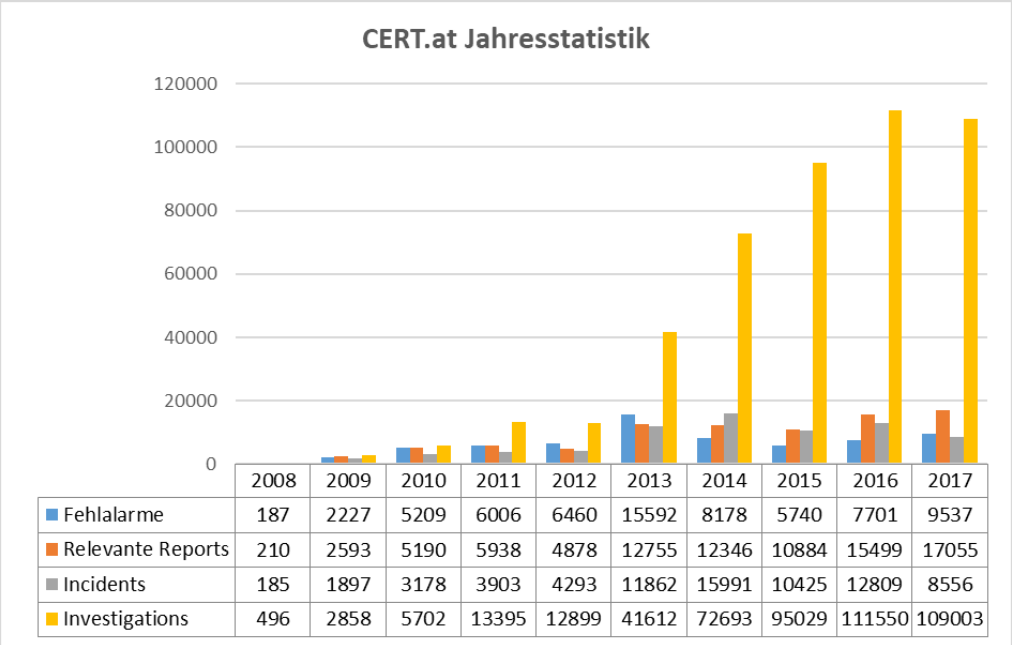
- **Recognition of the area of impact**; incidents may have various impacts on different CSIRTS, since they can be limited to sectors or to special types of victims, whereas some may underlie political reasons e.g. in the case of elections or may have criminal causes such as blackmail.
- **Familiarization with the kind of events that lead to incidents**
- **Enhanced understanding of incident taxonomy by decision makers**
- **Access to up-to-date information**
- **Application of standards**
- **Different treatment of confirmed and unconfirmed events**
- **Assurance of sensitivity**, i.e. information must be tagged using the traffic light protocol

ENISA, 2018a

As according to the NIS Directive (2016) “Member States', each country’s preparedness regarding the responding to incidents must be ensured by requiring them to be appropriately equipped, e.g. via a *Computer Security Incident Response Team* (CSIRT)” (Cert.at, 2019). For this reason, Austria also brought a national CERT into force – cert.at. This computer emergency response team is the **primary contact for IT security**. Cert.at must be contacted in case of obligatory messages in case a sector specific CERT does not exist (Cert.at, 2019). Moreover, CERTS also serve as a **partner in the occasion of voluntary messages**. Even so, Cert.at is the national CERT and always keeping a good cooperation with the Austrian governmental authorities, confidentiality is ranked first. This implies that information is never forwarded without permission, to guarantee for the highest security and confidentiality possible (Cert.at, 2019).

Furthermore, sector specific CERTs are being designed. Worth mentioning here is the energy CERT, which forms the response team for the Austrian Electricity and Natural Gas sector. This CERT represents the *single point of contact* for this sector and reports directly to the national authorities and its main duties are the strengthening of cybersecurity and to raise awareness (Cert.at, 2019).

All these measures are reasons for the existence of the NIS law. The following graph displays the illustration of the significance of incident reporting ascending incident statistics:



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Fehlalarme	187	2227	5209	6006	6460	15592	8178	5740	7701	9537
Relevante Reports	210	2593	5190	5938	4878	12755	12346	10884	15499	17055
Incidents	185	1897	3178	3903	4293	11862	15991	10425	12809	8556
Investigations	496	2858	5702	13395	12899	41612	72693	95029	111550	109003

Figure 5: Cert Statistics

In the case of noncompliance, administrative penalty proceedings will be initiated; The penalty charge is 50.000 euros, in case of recurrence 100.000 euros (NISG, 2016, §26).

2.8 ENISA' Support

The *European Union Agency for Cybersecurity* (ENISA) has been highly conducive to EU cybersecurity policy since 2004 (ENISA, 2019a). The ENISA encourages and supports EU member states and stakeholders to react against the increasing number of cybersecurity incidents in order to enable the proper functioning of the digital market.

The agency closely collaborates with EU's member states and the private sector in terms of providing advice and solutions. This assistance involves inter alia:

- Pan-European (concerning all European countries) cybersecurity operations

- Deployment and assessment of national cybersecurity policies
- CSIRTs cooperation and capacity building
- Addressing of data protection issues, enhancement of privacy technologies and examination of the cyber threat landscape

ENISA, 2019a

Furthermore, ENISA contributes to the development and adoption of the EU's policy and law regarding the field of *network and information security* (NIS) (ENISA, 2019a).

ENISA has published the *technical guideline for minimum-security measures* in order to guide national regulators on the security measures to be considered in the assessment of compliance to the *Telecommunications Framework Directive*. Article 13a of this directive requires network and service providers to take proper security measures to guarantee security and integrity of networks (Framework Directive, 2002).

National regulators from different EU countries were scraped together in various workshops and meetings in order to develop the '*Technical guideline for Minimum security Measures'*. Thus, a cornerstone of the NIS could be formed (ENISA,2018).

3 Methodology

In the following part, some deeper insight into the methodology used will be provided by further elucidation of the structure and construction of this research.
Hereby, the different steps necessary for the construction process are displayed in the figure below.

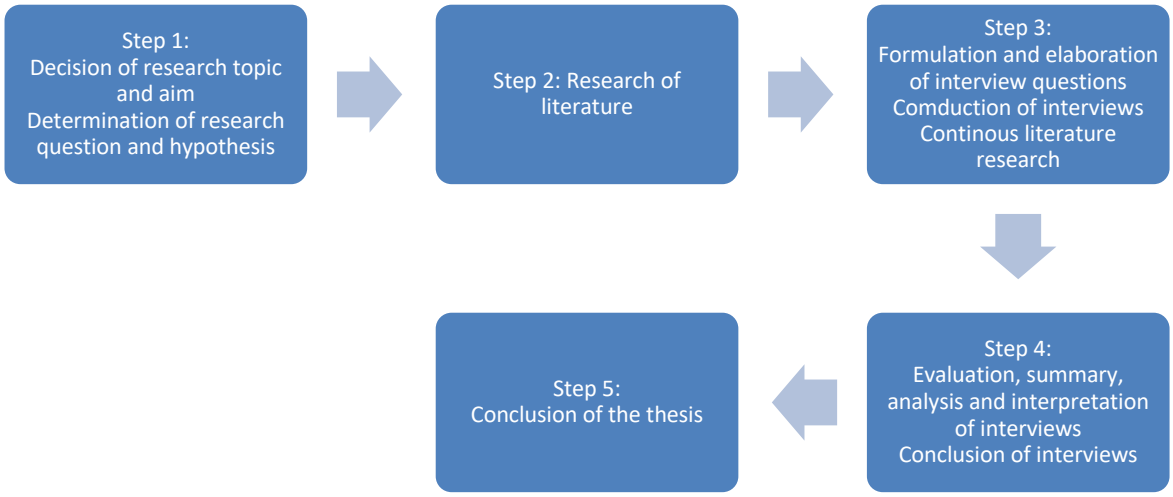


Figure 6: Structure of the Thesis

3.1 Aim

In order to satisfy the main aim of this thesis “economic and/or organizational impacts of the NIS law on Austrian operators of essential services” the research process was divided into two phases. Part 1 dealt with the legal process, as the NIS law is base of discussion for this bachelor thesis. Secondly, the researcher described how the data collection was planned to conduct the qualitative research.

3.2 Research Design

According to Bogner (2009, p. 2) “Firstly, in relative terms, talking to experts, people who have extensive knowledge in a particular field, in the exploratory phase of a

project is a more efficient and concentrated method of gathering data than, for instance, participatory observation or systematic quantitative surveys“, the explorative method of the conduction of interviews according to a qualitative thematic analysis is elected.

According to Bogner, three different types of interviews are available:

- Exploratory interviews
- Systemizing interviews
- Theory generating interviews

Bogner, 2009

While *systemizing interviews* are frequently used for the reconstruction of already known artefacts, *theory generating interviews* not only apply the expert´s knowledge but are also based on the interaction between the expert and the interviewer. However, since the topic of minimum-security standards, which are controlled by law, is rather recent, the conduction of exploratory interviews may well be the best solution in a relatively unknown field. The researcher plans to start the interviews with members of public authorities, which could lead to a broader spectrum of the topic and could give access to experts in key positions (Bogner, 2009).

3.3 Unit of Analysis

In this research, there are two units of analysis, whereas the first unit is represented by the **literature research**. The second unit of analysis, **expert interviews**, was divided into three subcategories; **experts** who were **participants in the legislation process**, an **advocacy group** who supported member firms affected by the NIS law during the implementation phase, and **security experts** who are **employees of critical infrastructure.** The legal research process followed Doctrinal research — “Research which provides a systematic exposition of the rules governing a particular legal category, analyses the relationship between rules, explains areas of difficulty and, perhaps, predicts future developments” (Duncan & Hutchinson 2012, p. 101). Beginning with the facts, the researcher started with primary resources, which was legislation, namely the NIS Directive and Austrian NIS law, in order to ensure all that relevant facts are clearly understood. This directly led to the second step – the

definition of the issues that concur with all the facts collected. All these matters induced the third step "law/legal" research. This time, secondary sources were utilized e.g. the examination of the law, reviews, journals and articles. As the final step, analysis of the research gathered was conducted in order to be able to start on the qualitative approach. In this case the method of interviewing experts was used, whereby this unit of work was split into two sections:

- Interviewing experts of law enforcement agencies
- Interviewing experts of operators of essential services

3.4 Data Collection and Analysis

For the analysis of data, a thematic analysis according to Braun & Clarke (2012) was used. This method teaches a mechanic to analyse data systematically in a way to fulfil a broader issue. In addition, it ensures accessibility and all the flexibility needed by giving the choice what form to use. The researcher had decided on an *inductive method*, which is a bottom up approach. However, reality shows that very often a combination of deductive and inductive methods is used, but "An inductive approach to data coding and analysis is a 'bottom up' approach, and is driven by what is in the data. What this means is that the codes and themes derive from the content of the data themselves – so that what is 'mapped' by the researcher during analysis closely matches the content of the data." (Braun & Clarke 2012, p 2).

Since all subjects concerning the NIS law are predominantly unfamiliar to the broad mass of people, qualitative research must be applied in this case which implies the conduction of expert interviews. According to Bogner (2009), experts are commonly viewed as so-called *crystallization points* within the process of gathering data, since they are essential for the provision of practical insider knowledge. The conduction of expert interviews serves the aim to represent a broader field of players, whereby the expert serves as a surrogate for them. Hence, the method applied is *inductive*, i.e. statements, claims, propositions, predictions made by a limited number of participants are applied generally and represent the broader mass (Bogner, 2009).

As a first step, the researcher has to get familiar with the data, read the notes carefully and start thinking (Braun & Clarke 2012). This forms a stable base for the second step

– the generation of initial codes, which are rather descriptive than interpretative. Attention has to be paid according to the research question, especially under which perspective interviews have to be read. In order to answer the research question of this thesis, the content of the interview is of significant importance, but not the reactions of the interviewee. Already during the subscription of the interviews, the most essential paragraphs became obvious. Nevertheless, whatever seems to be of relevance, in this case, all interviews, has to be coded (Braun & Clarke 2012).

The next step is called searching for themes, which is the transition from codes to themes (Braun & Clarke 2012). This process was supported by the use categories, i.e. data will be split into small units of meaning in order to work towards a concept. The units will be defined by asking relevant questions such as:

- Which actors participate
- Which phenomena exist
- Which impacts do we see
- Which strategies are used
- What are the consequences

Braun & Clarke 2012

When reviewing the coded data, the researcher had to ensure to receive a meaningful pattern where similarity and overlaps were avoided (Braun & Clarke 2012). On one hand, information gathered during the interviews was condensed and redundant information eliminated. Thereafter, themes were set into relations in order to create a relational model. This technique supports the recognition of causes, strategies and consequences and show how themes work together. The target of this phase was to receive a thematic map.

Thereafter, quality of the data reviewed had to be raised in a recursive process. The researcher checked whether the themes work, whether the boundaries were set accordingly, whether there was sufficient data and whether the data is diverse. The purpose is to receive a set of themes in relation to the research question as well as to receive a broad picture considering perspectives of different parties concerned. Finally, she reached the last phase – definition and naming of themes. This is the deep analytic phase in which the story is presented and analysed again in a recursive

matter. Data had to be interpreted, analysed and reported, until the story was complete (Braun & Clarke 2012).

"Finally, a clear and systematic analytic process can increase transparency in qualitative research. In order to reduce the opacity of qualitative data analysis, methodology sections must be more specific than "I analysed the data using qualitative software'" (Deterding, 2018, p.26). In order to do so, literature was used again to compare the researcher's findings to already existing theories. In parallel, since the NIS law is rather new in place, some more recent research was expected to exist at this stage already, which would further validate the findings (Creswell 2003, p. 207-215). Moreover, if certain facts were mentioned repeatedly during the several interviews, they proof to be valid. It was expected to find the key effects driven by this law e.g. raised awareness, sensitisation of companies and reasonable expenses into security. Moreover, the researcher was certain that by questioning such a broad spectrum, many details, which had not been considered of, would reveal.

The primary findings for this empiric research were based on face-to-face expert interviews. Through the application of this qualitative approach, detailed information could be gathered, as well as the possibility to scrutinize certain given answers is provided. The decision regarding the location of the interviews will was up to the experts. A semi-structured guideline was provided in German and in English language. Nevertheless, all interviews were held in German language. The guideline was sent out prior to the interviews if requested. Applying the semi-structured guideline, only specific research questions were defined in advance, but no possible answers given. This method just narrows the potential answers to relevant ones according to the research subject. At the start of the interview, all the research facts and issues were explained. Due to traceability, all interviews were recorded after the expert approved. Furthermore, experts were asked whether he or she wants to remain anonymous. If otherwise, the expert was also requested to introduce him- or herself.

3.5 Participants

Since the NIS law is not a field the broad mass of people is familiar with, experts of this field had to be approached in order to study the impacts of the NIS law on operators of essential services in more detail. The NIS law addresses a very narrow

field. Thus, the ones who are familiar with it are mainly authorities, Computer Emergency Response Teams and operators of essential services. The law only focuses on the security of big critical infrastructure and its operators and does not consider small or medium-sized companies or even single people. Therefore, in order to study the impacts of the NIS law, people who were part in the legislation and elaboration process of the law, as well as an advocacy group for operators of essential services and employees of critical infrastructure were approached and interviewed by the researcher. This second unit of analysis, the expert interviews, was split into these three categories in order to get a complete and harmonised picture by taking various different viewpoints and opinions from different parties operating in different positions into consideration. By doing so, the researcher aimed to exclude biases by studying the impacts of the NIS law from at least three different perspectives.

As the first step interviews with experts from the public authority were conducted. Both of them, Gernot Goluch and Erik Gwehenberger, are employees of the Ministry of constitution protection and counterterrorism and were involved in the legislation and elaboration process of the NIS law.

In order to receive a list of digital service providers, who were contacted via email, the Ministry of Interior was approached. However, the election and appointment of digital service providers are still in progress. The NIS Directive being the originator for the Austria NIS law under Union law intends to be implemented in full harmonisation, i.e. there was no leeway in the transposition process for the implementation of the guidelines set by the NIS Directive regarding scope of application and duties. Contrary to operators of essential services who are informed by the Federal Chancellery, digital service providers have to identify themselves and assess, based on the characteristics defined by the NIS Directive and the NIS law, whether they are digital service providers and must therefore fulfil the corresponding duties, i.e. implementation of safety measures and duty to report incidents. Thus, a valid list of digital service providers cannot be provided (Gwehenberger, Ministry of Interior 2019).

In order to actually receive a broad picture of the current situation regarding the NIS law in Austria, the Verband der Öffentlichen Wirtschaft und Gemeinwirtschaft Österreich (VÖWG) serving as an advocacy group for operators of essential services, and the operators themselves were approached and interviewed by the researcher.

The goal, again heavily supporting the main aim of the study, was to get insight information about their experiences with the NIS law, as well as on their feelings and perceptions.

3.5.1 Selection Criteria

According to Bogner (2009) expert knowledge is seen "as an 'analytical construction' and, at the same time, incorporates the expert's 'formative power'. Therefore, expert interviews are an essential part of this thesis. Accordingly, the conception of the interviews as well as the selection of the interview partners were carried out with great care. These two topics will therefore be given special attention in the following section.

3.5.2 Construction of questionnaire

The basis of the interview concept is the fact that information gained from interviews can be selective and sometimes contradictory in individual cases. Therefore, it is not only useful but also necessary to conduct several interviews with the same questions in order to get a complete picture of the situation (cf. Bogner, Littig, Menz 2014, p. 72

Good question always starts with ideas and the main question 'What do I want to know?'. In the beginning, the broad question exists, which leads to a series of more specific questions. This broad question always stays in the focus of the researcher in order neither to get a 'tunnel vision' nor to get off the point (Clegg & Stevenson, 2013). Building on this insight, the complex of topics dealt with in interviews in the context of this study have always been secured several times. The interviews followed - apart from one exception - a uniform, tripartite structure.

- Questions about the person, the area of responsibility and the organisation of the interviewee
- Questions on the implementation process and the cooperation between authorities and operators of essential services
- Questions about changes, improvements and eventual burdens caused by the NIS

The structure and the design of the interviews follows the structure of the present study. The questions on person, field of activity and organisation primarily serve as an

easy introduction to the interview situation and an overview of the background of the person. This knowledge also serves as a basis for the respective parts of this thesis. During the interviews, the questions were posed all posed in the same manner. All other queries represent the persons knowledge and personal experiences, expectations or opinions on the respective field and were further grouped into the categories:

- Implementation of the NIS law
- Cooperation
- Minimum-security standards
- Incident reporting
- Organisational changes
- Personal opinion towards the EU's approach and the NIS law

The purpose of posing questions regarding the implementation of the NIS law was to get more detailed information about the proceedings of the still ongoing implementation process of the law, i.e. what has been realised already and where there is still work to being done, as well as to discover potential issues which arose during this process. In addition, the researcher questioned the purpose of the NIS law by asking about the improvements that are expected from it. Hence, the questions on the implementation of the NIS law asked were:

- In your opinion, how has the implementation of the NIS law proceeded so far?
- Does the NIS law meet your expectations? (If not, where does it deviate?)
- Was the implementation into national law realised as planned?
- Was gold plating carried out? / Was the target overshot?

The goal of asking the questions regarding the cooperation between the authorities, operators of essential services, Computer Emergency Response Teams, advocacy groups and potential other parties involved, was to find out to what extend opinions of all parties affected by the NIS law were not only considered during the law-making process but were given the possibility to contribute to the elaboration of the final law. Moreover, the researcher aimed to find out, how deliberately and frequently communication between these single parties takes place. Thus, the questions on cooperation were:

- When you think back to the law-making process, how would you assess the cooperation between the state and the economy?
- How is the cooperation with the economy (=operator of essential services) assessed from the authorities' point of view?
- How do you assess the cooperation with the authorities so far?
- What preparatory measures were taken with the industry involved?
- Are frequent sanctions to be feared?
- Is it to be feared that the cooperation with the economy will be weakened by such sanctions?
- Can the cooperation between the state and the economy be strengthened, or are negative influences of the NIS law noticeable?
- Can the cooperation between the state and the economy be enhanced by the obligation to report or are negative influences of the NIS Act noticeable?

In order to get a better understanding of the meaningfulness, purpose and benefits of the introduction of minimum-security standards, the authorities were approached with the following questions:

Minimum-Security Standards:

- What criteria were used to select the minimum-security standards?
- What criteria were used to define the threshold values?

All interviewees were asked the following queries regarding the reporting obligation in order to discover both positive and negative aspects that come along with it.

Reporting:

- In your opinion, does the reporting obligation contribute to get a better picture of the situation?
- Will the reporting obligation contribute to improving transparency?
- Can the cooperation between the state and the economy be enhanced by the obligation to report or are negative influences of the NIS Act noticeable?
- Are you afraid of the reporting obligation leading to negative headlines for your company?

Questions on organisational changes were posed to operators of essential services and the Verband der Öffentlichen Wirtschaft und Gemeinwirtschaft Österreich (VÖGW) in order to assess and eventually being able to quantify the expenses and efforts for operators of essential services caused by the implementation of the NIS law. Hereby, it was expected to identify whether all systems needed were already installed before the implementation as a preparatory measure or otherwise even regardless of the NIS law, as well as whether there is sufficient personnel with the respective know-how or if outsourcing had or has to be carried out, since all of these are factors that contribute to rising expenses. In addition, the researcher aimed to find out if any kind of structural changes within the firms had to be made, such as reassignment of the employees' job tasks, hiring of new or retraining of existing staff. In order to answer these queries, the questions regarding organisational changes were:

- Have there been any changes in the organisation of your company?
- Were new jobs created for this purpose?
- What improvements can be expected from the NIS law from your company's point of view?
- How do you assess the financial expenditure caused by the NIS Act?
- Is it to be feared that the cooperation with the economy will be weakened by sanctions?
- Were any kind of preparatory measures taken in your company – before the NIS became effective?

Questions on the interviewees' personal opinions towards the EU's approach and the NIS law were posed to discover their feelings towards the NIS-law. This served the purpose of getting a deeper understanding of what the law is actually good for in practice, to further distinguish where it is helpful and where it might even be unnecessary. In addition, the researcher aimed to find out more about what the NIS law cannot cover, potential issues which need to be solved in the future and how the law should maybe be adapted. For this reason, the questions regarding the interviewees' personal opinions asked were:

- What improvements can be expected from the NIS law?
- Do you support the EU's approach to regulate security, especially cyber-security, by law?
- Does the NIS law meet your expectations?

However, it has to be said that personal opinions and feelings towards the NIS law new regulations were apparent throughout the interviews and stated in many answers.

All of the interviewees agreed on the publication of the interviews. However, one of the operators insisted to remain anonymous. Neither his name, nor the organisation may be mentioned in this thesis. Furthermore, the researcher has to ensure that it is impossible to draw conclusions on the organisation affected. Thus, detailed information regarding systems or location will not be provided either. It is well understandable that the operator wants to stay anonymous, since the NIS law is a rather sensitive topic. On the one hand, the appointment of firms to operators of essential services is still in progress, i.e. not all firms that will be affected by the law have already been notified. On the other hand, no published list of operators of essential services or critical infrastructure exists, which implies that only operators themselves know after having received the notification. Obviously, more people than the ones interviewed by the researcher bother with the NIS law. However, the intention was the provision of a complete and harmonised picture by getting the views and opinions from three different parties, as already elucidated before. In addition, the NIS law is still a very recent topic, which implies that there is little experience regarding its implementation. Therefore, it is difficult to make statements about that and a topic that may be considered in the future again.

4 Summary of Interviews

Category	Name	Organisation	Position
Authorities			
	E. Gwehenberger	Ministry of Constitution Protection and Counterterrorism	
	G. Goluch	Ministry of Constitution Protection and Counterterrorism	
Operators			
	Anonymus - known by supervisor	Anonymus - known by supervisor	Anonymus - known by supervisor
	A. Graf	Salzburger Landeskliniken	Chief Information Security Officer
	W. Plessl	Hewlett Packard Enterprise	
Advocacy Groups			
	H. Maier-de Kruijff	Verband der öffentlichen Wirtschaft und Gemeinwirtschaft Österreichs	Managing Director

Table 3: Participants of Interviews

The researcher aimed to consider the opinions of the different parties affected by the NIS law equally. However, advocacy groups or other sort of interest representatives which consult operators of essential services rarely exist, since this task is primarily

fulfilled by the authorities. In addition, the operators approached by the researcher all work for different organisations and operate in different sectors of critical infrastructure, which also offered the opportunity view the topic of their experiences with the NIS law from different perspectives.

In order to answer the main question of this thesis, the economic and organisational impacts on operators of essential services, in addition to the results of the document analysis already collected, answers from different points of view were available, which ultimately provided well-founded results on the basis of a comparative content analysis of the statements.

Operators of essential services have to be audited once every three years and are obliged to report serious incidents to the authorities. In addition to that, they are not only given the possibility but welcomed to also do voluntary reports, i.e. to communicate near misses in order to let others learn from their mistakes.

Investments will come along according to the audits. Not only audits once every three years must be funded, but also companies are obliged to react to every finding. On the one hand, it was reported that further investments into their cybersecurity had and have to be taken by operators of essential services since the enforcement of NIS law. Additional capital expenditures did not primarily occur due to increases in the workforce, but due to consultants that had to be paid and personnel that had to be retrained at a cost of several working days. Also, potential investments that have to be taken in the future are feared to be very high.

5 Interpretation of Interviews

5.1 Implementation of the NIS law

In your opinion, how has the implementation of the NIS law proceeded so far?

Goluch	- very positive because all parties involved cooperated very well - meet representatives from every sector
Gwehenberger	- very positive so far - is good communication with the affected companies of the respective sectors - very good cooperation with the Federal Chancellery
Graf	- Basically good. - Authority eager to inform - Authority has also approached us in the form of information sessions. - now becoming interesting, with regard to the specific definitions of essential services and, ultimately, of safety precautions - still a lot to be agreed on here, and, above all, specific industry know-how is needed. For example, it is easier to determine whether a service is available or not in the case of an electricity supplier. In other words, there is electricity or there is no electricity. That can be clearly defined. It can also be clearly proven. In the case of a hospital operator, it is much more complex, because, for example, an essential service such as the supply in a shock room is also available if an IT system is not available, and here it is important to find a good, common path with the authority. In particular, the inspection catalogue must then contain this accordingly and also be delimited.
Plessl	- happened rather quietly - not a wow-effect, which was supported by the media, but the law was activated and my presentation is that now you can observe and see how the whole thing starts and how it is used.
Anonymous	- waiting to receive the decree - of course we know which of our systems in are in principle subject to the law, yes, but there has not yet been any notification. - Once the decree has been issued, the company will then have three years by law to choose a qualified body to audit us as a company, which will then carry out the audit. - the NIS law has not yet landed properly, the notification is still missing.

Maier-de Kruijff	- implementation by our member companies has gone very well so far. - Many of our member companies are very well positioned in the cyber-security sector and have therefore already fulfilled many of the requirements before the NIS Act was enacted. - Furthermore, some of the companies have already been subject to similar regulations in other directives.

Table 4: Feedback on implementation

From the answers received differences in the interviewees' perceptions about the proceedings of the implementation process can be detected. From the authorities point of view, exchange of information and communication was reported to be fulfilled in an excellent manner. However, the operators' responses show varying degrees of agreement on these matters, i.e. some of them reported great involvement and communication, whereas others still have more of a wait-and-see approach.

Was the implementation into national law realised as planned?

Goluch	- Yes, if you ignore the temporal component - should have been implemented in Mai, 2018 - was fully transposed at end of December 2018
Gwehenberger	- In terms of timing, no. It could not be implemented in a timely manner because the NIS-Directive provided that by 9th May 2018, it should have been transposed into national law. Austria did not do that until the end of 2018. - This delay in time was the only thing.

Table 5: Feedback on realization of implementation

As reported by the authorities, the realization of the NIS-law was fulfilled as planned, except for a delay in time of half a year.

Was gold plating carried out? / Was the target overshot?

Goluch	- No, not in Austria. - adopted exactly the sectors of the EU directive - only thing that has happened in Austria is that the public administration has also committed to stick to the law. The state says "I have to obey the law myself, if I ask of the critical infrastructures to do so." Certainly, that makes sense… point of discussion for the future, if other sectors should be integrated in a few years that are not within the scope of application now (simplest example - drinking water is present, but not wastewater)

Gwehenberger	- Goldplating has never been an issue.

Table 6: Feedback on goldplating

As opposed to some other laws, gold plating or overshooting of the target were stated to have never been as issue.

Conclusion on questions regarding the implementation process of the NIS law:

All of the interviewees reported that the implementation process of the NIS law has gone well. The NIS was incorporated into national law in December 2018. However, the transposition should have been completed by 9th May 2018. As reported by the authorities, gold plating has never been an issue in Austria, i.e. the target was not undesirably overshot. However, the integration of additional sectors may well be of concern in the future. Furthermore, all parties involved reported that operators of essential services and CERTs were invited to several sector talks by the authorities in which they were given the opportunity to actively contribute to the creation of the final law. However, since the NIS law is still rather recent, not all operators of essential services have been identified and are still waiting to receive a formal decree by the authorities. Furthermore, as already mentioned, operators show lower degrees of enthusiasm regarding the actual involvement in the law-making process than the authorities.

5.2 Cooperation

When you think back to the law-making process, how would you assess the cooperation between the state and the economy?

Goluch	- …very good and strong cooperation between the economy and the authorities, on the one hand the Inner Ministry, but also the Federal Chancellery.
Gwehenberger	- excellent example of how you can involve the economy in the process of creating a law. - …not the usual case in terms of how that happened and it would be desirable if that was done in other areas as well. (several rounds of so-called sectoral talks in the course of the legislative process where at that time potentially affected companies were invited, sector representatives, sector associations, departments, other departments that are responsible for possible companies, for example the BMVIT, the Ministry of Transport for the ÖMV, ASFINAG and so on. They really tried to work out a balanced solution together or

	to get input from the respective sectors in order to work out a balanced solution in order to get a correspondingly presentable result in the end.)
Graf	- I wasn't really involved in the law-making process and can't really say anything about that now.
Plessl	- good communication - sector talks should have taken place earlier and in more intense way
Anonymous	- personally cannot say anything about that because I was in a different position at that time - my boss was involved - our organisation was involved in the sector talks - of course - we know each other in the sector between companies and authorities - we know and we value each other - relatively good cooperation, where we have been able to contribute our point of view and which has been taken into account as far as it makes sense. - in principle, we have worked together well - the whole development in Austria from the law and then the regulation in further consequence.
Maier-de Kruijff	- normal legislative process in which we, as well as some of our member companies, used the opportunity to submit comments on the draft.

Table 7: Assessment of cooperation

Again, slight variances along the interviewees' opinions regarding corporation and communication can be seen from their responses. On the one hand, the authorities said to be highly satisfied about the excellent collaboration and incorporating opinions of all parties concerned, again emphasising on the involvement of the industry within the sector talks. On the other hand, the operators and the advocacy group show a more restrained attitude but still mostly reported good and reasonable communication.

How is the cooperation with the economy (=operator of essential services) assessed from the authorities' point of view?

Goluch	– very positive (All interest groups, individual companies, or representatives of the authorities communicated at the same level. Years ago, some colleagues from another Department have already started with the conduction of sector meetings where all parties involved where invited and where we explained the rules and how they should be implemented)

	– ongoing cooperation; everything works well – very lively exchange of ideas now
Gwehenberger	- most of the sectors are currently under investigation. Only the sector drinking water is ascertained. This means that this area of investigation is of the Chancellor's responsibility determined by the Federal Chancellery through official channels in the meantime by an official decision. This means that they received the status of operators of essential services according to the NIS law.

Table 8: Assessment of authorities point of view

How do you assess the cooperation with the authorities so far?

Graf	- authorities eager to inform - involved in sector talks
Plessl	- cooperation basically works well. I would have only wished that we were involved in all the relevant contents earlier. - Sector talks should have taken place earlier, maybe in a more intensive way
Anonymous	- Relatively good cooperation
Maier-de Kruijff	- My association cooperates very well with the responsible authorities and has also been able to organise workshops with employees of the responsible authorities for member companies subject to the NIS Act.

Table 9: Assessment of cooperation from operator's point of view

What preparatory measures were taken with the industry involved?

Goluch	- sectoral discussions - statements received from the economy on the part of the legislature have all been processed. There was not a single opinion that was not considered - if you look at the law, before the opinion process as well as after it, really major changes were done there. Positive changes, reported by the business community, which were registered by the public.
Gwehenberger	- sector talks - bilateral talks, respectively trilateral talks between the BMI, Federal Chancellery and possibly affected companies, or with the Chamber of Commerce and so on - business community and the private sector has been sufficiently informed

Graf	- sector talks - information meetings
Plessl	- sector talks
Anonymous	- sector talks - consideration of our company's stance
Maier-de Kruijff	X

Table 10: Preparatory measures

Are frequent sanctions to be feared?

Goluch	I don't think so. (because these are big companies, which have to and want to take care of the topic in a positive way. we in Austria are going the official way anyway: first consultation and then punishment) most problems can be solved in good cooperation, but of course you have to be realistic when we talk about 100/150 companies, there will be sanctions at some point. This is the case with almost every law and they will probably be judged by the legal authorities and then there would be a decision. I expect this to be a rare and would be surprised if otherwise.
Gwehenberger	Hopefully not. Because it is an administrative matter and because the NIS directive also allows for it, there are sanctions at the end of the NIS law. We hope that there will be no need to use these penalties, because we believe in good cooperation between business and authorities and it will not come to that.
Graf	*X*
Plessl	*X*
Anonymous	- *No, definitely not.* - *Our systems are state of the art. We are well equipped.* - *There are no sanctions at all.* - *Of course, these fears have been present, even before there NIS, in regards to what a strategic or critical infrastructure is.*
Maier-de Kruijff	*X*

Table 11: Fear of sanctions

Would the cooperation with the economy be weakened by such sanctions?

Goluch	- Yes, double-edged. - If the cooperation was weakened for whatever reason, or if the cooperation would not work anymore, then this would inevitably lead to a higher number of sanctions. - where it will be necessary to have follow-up consultation, follow-up cooperation, there will certainly have to be the possibility of sanctions
Gwehenberger	- danger exists at least theoretically, but the companies are aware - common practice in administrative matters - not a new system that is being established - penalties are also set within a framework that is understandable - a lot that would need to happen to actually have a penalty payment, because there are certain mechanisms in the law in order to give the companies concerned the opportunity to compensate for abuses before a penalty is even imposed.
Graf	- depends on how the authorities will handle that. We will see.
Plessl	- Sanctions are never good - proponent of consensus. Yes, we love cooperation. We promote cooperation. Only together are we strong and I want to keep it that way.
Anonymous	- There are no sanctions to fear for us. We are well equipped - systems are state of the art - But nobody is safe from cyber attacks and then reporting would of course have to be done - external influences can never be excluded - discussion about this, so there will be additional work, but it has to be said that this has not yet been approved in principle, so it has not yet been achieved. In fact, generally speaking, of course, due to the additional threat of cybersecurity, yes, is of course an additional expense against for companies, yes, but that is independent of the NIS legislation.
Maier-de Kruijff	- No, I don't think so, because companies want to keep sanctions low and good cooperation is the best way to influence them. - The sanctions in the NIS Act are necessary as a means of exerting pressure on companies to implement the committed security requirements.

Table 12: Impaired cooperation by sanctions

Can the cooperation between the state and the economy be strengthened, or are negative influences of the NIS law noticeable?

Goluch	- So far, I don't see any. But it is only now beginning to be operational. - Everything is still within the stage of construction. - But I believe that at the moment it is pointing in a positive direction. - …have to be careful that it stays that way and keep working on it.
Gwehenberger	- no negative effects noticeable yet. - hope that the cooperation will simply be maintained - We also really try to approach the affected companies in a cooperative way
Graf	- Well, that depends; - in principle, I do believe that cooperation between the state and the economy can be strengthened. How this is then lived out in practice depends, of course, on how the authority deals with it. - I believe that it will be important to define and communicate a good network of national and state officials in the event of a security incident…for example, about the area of state crisis and disaster management, where the states also have competence, and I believe that this must also be well networked and coordinated to determine who's turn it it.
Plessl	- Negative influences are not known to me at the moment.
Anonymous	- Processes are being optimised - Processes being harmonised - Better understanding of the organisation and the whole topic - form this awareness - what are our critical processes, critical systems - how do we protect these systems
Maier-de Kruijff	- can improve cooperation between the state and the economy. - I didn't observe that the cooperation between our member companies with the state is negatively affected

Table 13: Influences of the NIS law on cooperations

All of the interviewees stated that the communication between the industry and the operators is enhanced, not only due to the NIS law and the obligation to report, but also due to the authorities' eagerness to inform and cooperate. Furthermore, optimization and harmonization of various processes are some positive side effects that were reported to come along with the implementation of the NIS law. None of the interviewees reported to have experienced any negative effects from the law.

Conclusion on questions regarding cooperation:

Cooperation with the Federal Chancellery, CERTs and operators of critical infrastructure was assessed to be highly desirable by the authorities, mostly due to the fact that all parties concerned were actively involved in the implementation of the law and constantly having all opinions considered. Not only by holding the sector meetings, but also by organising various workshops and information meetings, the authorities were eager to inform, invite to participate, and educate employees of operators of essential services. These efforts were also appreciated by the respective firms and cooperation was rated to be good.
None of the interviewees reported to be feared of frequent sanctions to occur, since operators of essential services are big firms, which have always been eager to handle sensitive issues in a proper manner. Moreover, the authorities are convinced to be able to solve the majority of issues in good cooperation without having to impose many penalties. Nevertheless, sanctions will occur at some point, but very likely not too frequently as sanctions are common practice for administrative manners. However, if frequent sanctions were issued at some point, the cooperation would suffer, which would again lead to higher numbers of sanctions. This is expected to be a rare case, since companies are given the possibility to compensate for minor abuses of the law before penalties get imposed. In any case, sanctions in the NIS Act were stated to be necessary as a means of exerting pressure on companies to implement the committed security requirements. None of the interviewees has noticed any negative effects of the NIS law. In fact, it was reported that the law influences cooperation among the parties involved, awareness of cyber-threats and is a driver for process optimisation and harmonisation.

5.3 Minimum-Security Standards:

What criteria were used to select the minimum-security standards?

Goluch	- very much attached to the European guidelines…hundreds of standards that deal with cyber-security. - NIS Working Group of the Commission just issued a paper in which these security measures were described. - in principle we have taken these security measures and written into the national regulation. - description of the measures already came strongly from us, we didn't translate and adopt everything one-to-one, but rather looked through it, perhaps applying stricter standards here and there.

Gwehenberger	- a lot of considerations on the European level, but this led to the fact that there is a so-called NIS Cooperation Group, a body in which the member states are represented, which deals with the topic of NIS and cyber-security. - They also developed a paper in cooperation with the ENISA, where established standards, which are currently in use…more or less in a mapping table evaluated and in addition to there was also a docent, where individual security measures were described and then taken from this and austrophied. That means more or less adopted, but the one or the other point was specifically adapted.

Table 14: Criteria for selection of minimum-security standards

What criteria were used to define the threshold values?

Goluch	- We had ideas and templates, what should adhere to. The thresholds, that was done by the Federal Chancellery, but we were strongly involved. - In principle, we sat down with the operators and sectors and really thought it through together: what is a reasonable threshold value for sectors A, B, C, D and did the same also for sub-sectors. In other words, this was done together with the industry. Mostly it is the number of the population, so how many people are affected or the time factor. But that is really totally different. You can also read that in the NIS regulation. It is partly different for some sub-sectors, for some sectors completely different. Sometimes it is user hours, sometimes it is a pure time component, sometimes it is metering points in the electricity sector for example and so on.
Gwehenberger	- several types of thresholds: -thresholds for identifying whether one is an operator of essential services at all -thresholds that determine when an incident has reached a certain quality, is therefore a so-called security incident, and therefore a mandatory report must be made - tried to be established in the context of these sectoral talks and the regular exchange of information with the industry, and was then incorporated into the NIS regulation

Table 15: Criteria for threshhold values

Conclusion on questions regarding minimum-security standards:

The minimum-security standards, issued in a paper by the NIS Working Group of the European Commission, are very much attached to the European guidelines which are

hundreds of standards that deal with cyber-security. These measures were adopted and written into the national regulation, whereas the description of the measures was adapted by the Austrian authorities, applying stricter standards at some points, not simply translated and adopted one-to-one. and applying stricter standards here and there.

The definition of the criteria of the threshold values was done by the Federal Chancellery, which was provided with ideas and templates to adhere to by the Commission. However, the Inner Ministry was also strongly involved and again invited potential operators of essential services to participate in the development of the threshold values. The goal was to work out and define reasonable thresholds for each sector and sub-sector, again having all parties incorporated. Resultingly, two types of thresholds were set:

1. Thresholds for the identification of whether a company is an operator of essential services
2. Thresholds that determine when an incident has reached a certain quality and is therefore a so-called security incident which must be reported

5.4 Reporting:

In your opinion, does the reporting obligation contribute to get a better picture of the situation?

Goluch	- There are two. There is the mandatory reporting and there is the voluntary reporting. - threshold values are very high; mandatory reporting is necessary if something really serious happens. That means if for instance electricity failed somewhere or ÖBB could not run any more trains through the area. So that's when the little man and woman on the street notice it. - hope and assume that we will not get too many obligatory reports. That would be bad, because that would mean that we have a huge problem in this area. - voluntary reports are much more important - the more voluntary reports we get, the more you cooperate, the more open you are, so also this Near Misses, so now something almost happened and I might report it anyway. If we manage to do that, then the situation will be much improved once again. - if this voluntary exchange of messages does not work, then you are dependent on the obligatory messages and hopefully there won't be many of them.

Gwehenberger	- Yes, absolutely - but obligation to report refers to cases that are really serious - we hope that the so-called right to volunteer will hopefully lead to a better overview, to a better picture of the situation in the individual sectors and also throughout Austria and, we must not forget, throughout Europe. That is the idea of really establishing a Union-wide system, where we can actually react quickly if security incidents occur.
Graf	- from the authorities' point of view, I guess so because I believe that companies have been rather reluctant so far and that a reporting requirement is also an obligation and that the number of notifications will therefore probably increase. - In principle, I do believe that cooperation between the state and the economy can be strengthened. How this is then lived in practice depends of course on how the authority will deal with it.
Plessl	- Yes. Definitely. I am one hundred percent convinced of that and would answer yes to that every time.
Anonymous	- Generally speaking, of course but the obligation to report would not be necessary - The NIS certainly is a milestone for companies, for operators of critical infrastructure - Authorities get a comprehensive overview of the market, about where critical infrastructure actually is present and where these companies are interrelated This is important - to view it systemically - view interdependencies between the industries and industry segments to receive a comprehensive picture in the end. - The NIS law in itself is certainly a good foundation, but it does not improve the situation - not substantially. Let's put it this way. Why? NIS has a very strong ITO view and therefore it has an extension to the typical company concept. - But on the whole - the situation would not be significantly improved from the point of view of the authorities.
Maier-de Kruijff	- Yes, the reporting obligation contributes to get a better picture. - Companies receive information about new attacks and especially about unknown types of attacks in a timely matter and can therefore protect themselves in a better way. - Furthermore, concealing incidents in companies is for more difficult than before.

Table 16: Reporting obligation

All parties agree that the obligation to report will contribute to receive a better picture of the situation. However, the number of benefits that will be experienced mostly depends on the number of voluntary reports made by operators of essential services. The authorities hope that this so-called "right to volunteer" will be used frequently in

order to open the possibilities to learn from near misses. The operators however do not seem to be very eager to communicate such minor disruptions straight to the government. Moreover, the question whether the obligation to report is redundant is still present.

Will the reporting obligation contribute to improving transparency?

Goluch	- Yes, in the closed circle of the addressees. - …as long as this remains, so to speak, transparent within the circle of the sectoral, the CERT, that is to say the computer emergency response team, authorities and operators, I believe that, firstly, we can certainly create more transparency and exchange of information, which is almost even more important. - Of course, not everything must be made public now. Understandably, companies are also afraid of this to happen, because if every report of a problem was published four hours later,…then we would of course have a problem.
Gwehenberger	- Argument has come up, that if this reporting channel or the reporting system is not regulated properly, then the reputation of the company could possibly be damaged, if before the responsible Ministry of the Interior possibly before the Ministry of the Interior receives the report that you are already reading in the newspaper, possibly with false information and so on and so on. - Paradigm shift in the meantime in that companies have realised that it is not the end of the world when an incident occurs: -the paradigm shift has moved from profiling to reacting -companies are more likely to be judged by how they react to an incident; how they interact with their customers... how they inform their customers...how they react to it and how they communicate. -So far, there is no company is a Fort Nox that you can't attack.
Graf	- From the authorities' point of view, I think so in any circumstance - Transparency is nothing I am too concerned about - It is important to me to be able to obtain information if, for example, another operator of an essential service has a security incident, because such an incident could also have an impact on our company and I hope that good communication between the players, i.e. between the operators, between the CERTs and operators, security incidents can be handled faster.
Plessl	- Certainly, yes.
Anonymous	- Rather consciousness
Maier-de Kruijff	- There is no improved transparency for us as an association.

	- It is certainly different for companies, because they are informed and warned about incidents.

Table 17: Reports and transparency

Generally speaking, all of the participants agree that the obligation to report can improve transparency, mainly for the authorities, but not for the operators or the advocacy group. However, an actual enhancement of transparency will depend on the number of voluntary reports the government receives, since complete failures are expected to be rare anyway.

Can the cooperation between the state and the economy be enhanced by the obligation to report or are negative influences of the NIS Act noticeable?

Goluch	- I know is, I heard someone from the Commission recently who said that they will have to amend, improve, strengthen and make the NIS directive stricter in the next few years anyway. - assume that either more sectors will be included or that certain requirements for the safety measures will be given by the EU or that for example the threshold values will be clearly defined. - Because that is the way things are now: each EU state is doing its own thing. There are those who set the thresholds very high. In Germany, for example, they have now set it rather low. This creates a bit of a rag rug. It would be a good idea to harmonise this after a few years because all sectors across borders are dependent on each other.
Gwehenberger	- no negative effects noticeable yet - hope that the cooperation will simply be maintained - try to approach the affected companies in a cooperative way
Graf	- X
Plessl	- Negative influences are not known to me at the moment.
Anonymous	- Process optimisation - Process harmonisation - Creating conscientiousness regarding what our critical systems are and how we can protect them best
Maier-de Kruijff	- The reporting obligation can improve cooperation between the state and the economy. - I didn't observe that the cooperation between our member companies with the state is negatively affected by the NIS Act. - Good cooperation is particularly necessary on an important issue such as security of network and information systems and I am sure that companies see it that way.

	- Both the regular exchange with the state and certain obligations formulated in the Nis Act have already been implemented before the NIS Act was enacted.

Table 18: Effects of obligation to report

Conclusion on questions regarding reporting:

There are two types of incident reporting, mandatory and obligatory reporting. The authorities assume and hope to only receive rare numbers of mandatory reports, since this would imply that serious failures or malfunctions do not take place frequently. Moreover, voluntary reports were stated to be of much greater significance because the more voluntary reports are made, the more is cooperated, the more open companies are and also report near misses, the better the situation will be. Resultantly, cooperation would be enhanced again, and other companies would be given the possibility to learn from other operators' behaviours, reactions or mistakes.

However, the argument has come up, that if this reporting channel or the reporting system was not regulated properly, companies' reputation could suffer. Therefore, it must be omitted that the media communicates incidents to the public, possibly also containing false information, even before the responsible Ministry of Interior receives the report. As reported by the authorities, there has been a paradigm shift in the end and companies have realised that the occurrence of an incident is not the end of the world. Companies have moved from profiling to reacting, since they are more likely to be judged by how they react to an incident and how they interact with their costumers or other parties affected by the incident. Furthermore, the authorities are well aware of the fact that a company that cannot be attacked does not exist so far and incidents can therefore always happen. Transparency was assessed to be enhanced by the obligation to report by the authorities and some operators of critical infrastructure. Two of the companies interviewed as well as the advocacy group stated that transparency would only be increased for the authorities, since they are the ones who receive the reports.

5.5 Organisational changes:

Have there been any changes in the organisation of your company?

Graf	- Independently of this, a project has also been started in which, among other things, the specifications of the NIS will also be incorporated.
Plessl	- Changes are constantly happening here, namely with regard to process and sequence control in the case of cyber-security incidents - created our own electronic education, where every HPE employee is obliged to take this course in order to create awareness of all the incidents that happen again, and this training content must be repeated in a detailed framework. A source of information is repeatedly sent out by this CISO at certain points, which, on the one hand, indicates where one has to react to it and, on the other hand, also sends out fake information, where one can then see whether the employees are implementing it. - emphasize the relevance again and to sharpen the awareness and this happens again and again. In other words, yes, training courses take place regularly to ensure that, if the need arises, there is controlled management and that we ourselves are always protected.
Anonymous	- No. Well, it is of course already the case that the NIS regulation makes us look more closely into certain areas. We are of course already looking at the NIS catalogue or the regulation on measures on certain points, which is what we have to look at. This starts with electronic access to systems and the systems must be handled accordingly, and in a restrictive manner...installations, physical access, access and access to installations. A management system for emergency crisis management must be established and suchlike. - The point is, thank God we have that all in place. - definitely need to look at this in some detail again and maybe adapt a few things where we are not yet ISO certified. - Needs to be looked at closer again in order to optimize management processes regarding risk and process management and whether the IT or ITO have to optimise them again - according to standards - Fundament is in place - perhaps needs to be adjusted here and there
Maier-de Kruijff	- No, because we are not subject to the NIS Act. - I am not aware that there have been any changes in member companies.

Table 19: Organisational changes

Were new jobs created for this purpose?

Graf	- no jobs specifically for the purpose of the NIS
Plessl	- we are an international company - accordingly initialised a position called Chief Security Officer who also ensures that such laws and rights and obligations can be implemented directly and locally. - not a dedicated worker as such, because that would not be one hundred percent capacity use somebody was dedicated to the NIS topic from Monday to Friday, from January to December, but a worker was created who has to serve several countries here. There is a network - Germany, Switzerland, Austria - of security officers who ensure that everything here is compliant. Such a role got created, but not a dedicated role in Austria.
Anonymous	- actually not, no. - Well, yes and no. - more and more positions are being established, such as IT or OT Security Officer, but not specifically due to the NIS but rather because of the issue of cybersecurity as a whole. Cybersecurity is an important topic, becoming ever more present, rated in the top five risks. - from the NIS legislation new jobs possibly, probably more from the corners qualified job - then consultants like TÜV for example, which act as a qualified body - in principle the companies can audit essential services. From this position, yes, there are of course additional business models and from this corner additional jobs were certainly created. So, the bottom line is definitely more jobs, yes.
Maier-de Kruijff	- No, not in my association. - In our affected member companies, the IT or ICT departments and employees have taken charge of this topic.

Table 20: Creation of new jobs

Do you fear negative headlines for your company due to the obligation to report?

Graf	- I hope not. - Would be counterproductive.
Plessl	- Partly I would say yes, because if there are incidents and you have to report them, that is always connected with a risk. - can't say yes and no - certainly a negative assessment for the institution that carries out the reporting. - always about media presence in the end. - In my opinion, voluntary reports happen rather reduced. - Compulsory reports are only made when there is really, I would say, imminent danger.

	- media effect everybody wants to avoid. That is really the insight I gain with customers when incidents happen.
Anonymous	- No. No. No, definitely not. Definitely not, because as a market participant we have obligations towards other market participants or competitors, or to report to our customers if we now carry out maintenance or similar. So it is a topic in the electricity sector, for example, just as it is in the gas supply sector, that if there is maintenance "ah maintenance - will be turned off" there must be corresponding remit reports to the other market participants that there will be a shortage in supply in the future or is currently present, in an emergency, for example. - So, this is really not an issue. Well, for me that is no more, no less, definitely not, no.
Maier-de Kruijff	- No, because my association is not subject to the NIS Act and therefore, we are not subject to the reporting obligation. - However, it can of course lead to negative headlines for companies who are subject to the NIS Act, if they don't deal with the topic of cyber-security and ignore the requirements of the NIS Act. - In the end, the reporting obligation may as well be an opportunity to learn from mistakes or carelessness of others.

Table 21: Fear of negative headlines

What improvements can be expected from the NIS law from your point of view?

Goluch	- almost obvious. - two main improvements: 1. the information, IT, cyber-security, whatever you want to call it, increases or, at least, will be unified in some sectors (Information security has actually been a private issue in many areas. Now these economies must be integrated according to the law. Thus, it is now no longer purely an economic issue but a social issue, a state-regulated issue) whole security area will experience a boost, simple due to the regulatory act. There is now even a law which requires companies to implement certain security measures. Such a thing did not exist before 2. NIS duty messages that will strengthen the exchange between economy, computer emergency response teams, authorities simply again, because it is now a legal basis exists. - Realistically, the population will not feel any impacts of the NIS. - As long as the law works well and incidents are properly reacted to, only the NIS' addressees of its obligations will know about it. (Thus, the broad mass of people will not feel know about it as long as everything works and will likely not

	report to feel much safer. This will take place at the level of the economy, the authorities and the cyber-security community.)
Gwehenberger	- affected companies now have the legal obligation to deal with cybersecurity (Hopefully that will also cause a cascade effect. This means that a state will hopefully emerge, i.e. the companies affected will be dedicated to the subject, but also, for example, small and medium-sized enterprises, which are not covered by the NIS law, ... it simply adds value to deal with cybersecurity from a business´ standpoint. Considering the exorbitant amounts of damage that can be caused by cyber-attacks or security incidents, it is obvious that the issue is becoming more important, both domestically and internationally)
Graf	- expect to be informed quickly in the event of threats affecting information security, uncomplicated communication with the respective offices in order to be able to react more quickly to information security incidents if necessary.
Plessl	- we ourselves have also been sensitized and through these sensitizations and the associated improved procedures and processes that have also resulted in improvements for us. - We really see the NIS law as a supplement to what we are doing in terms of the requirements that we have to meet as Hewlett Packard Enterprise. - That was already a satisfactory act, this law. - The question is just how much effort you have to invest in order to be able to really present a hundred percent complete solution. It's just an economic consideration of the interested parties.
Anonymous	- Process optimisation and harmonisation - Better awareness - Enhanced collaboration
Maier-de Kruijff	- My association is not affected, therefore I can't make an assessment.

Table 22: Expected improvements

How do you assess the financial expenditure caused by the NIS Act?

Graf	- financial outlay, i.e. the amounts specified in the law, which will be incurred by the operators of essential services, is far from realistic. In Germany, for example, there are subsidies for operators of essential services. This would also be very good for Austria, as the costs will certainly be considerable.

	How considerable they will be, depends on what the certified bodies now have and what kind of inspection catalogue they have - whether or not they are compliant with the standards. And as far as our regulations are concerned, the costs can be very high.
Plessl	- judged? That is difficult. - The expenses that arise here can't be quantified. We see it more as a proactive measure and try to prevent in case of damage, but it is difficult to evaluate it because it is difficult to put it into figures. You can only say that I am investing in the future in order avoid incidents and get the numbers to almost zero. The costs that arise from this are, let us say, manageable and profitable. - Cannot put into specific number
Anonymous	- Yes. Definitely, yes, because of course we do the risk analyses for areas for external partners in our company to prepare for this audit. This is definitely an additional expense also yes goes hand in hand. - effort of the consultant, of course, and then internally, of course, the hours that still occur in order to perform these analyses.
Maier-de Kruijff	- I have no insight into the financial expenditure of our member companies, so I can't answer this question.

Table 23: Assessment of financial expenditure

Were any kind of preparatory measures taken in your company – before the NIS became effective?

Graf	- in our organization, the confidentiality, integrity and availability of the data of our patients entrusted to us, even without NIS law, is an essential prerequisite for our company. These are the cornerstones of our mission, our corporate mission. Also the data entrusted to us by our employees. - Even before the NIS law, we had already taken measures and started a project as already mentioned. - Within the industry, we have started an ongoing coordination in preparation for the NIS law and its effects.
Plessl	- x
Anonymous	- x
Maier-de Kruijff	As we are a non-profit association and we are not an "operator of essential services", we are not subject to the NIS Act. Therefore, we have not taken any precautions.

Table 24: Preparations

Conclusion on questions regarding organisational changes:

All of the operators interviewed reported that the adaptations that had to be done in order to act in compliance with the NIS law were rather minor, since the systems needed had already been installed before, regardless of the NIS. Thus, only minor adjustments had to be done. However, systems must be updated constantly in order to protect oneself against the ever-increasing number of cyber-attacks. Furthermore, training and education of employees were stated to be of great significance in order to sharpen their awareness as well as to enhance their knowledge and skills. Hence, some of the companies have implemented training programmes and workshops specifically related to the NIS law.
None of the organisations reported to have additional staff hired because a full time worker dedicated to the NIS would simply not be working to capacity. However, positions such as Chief Executive, IT or OT Officers were initiated Officer who also ensure that such laws and rights and obligations can be implemented directly and locally. However, it was stated that within the companies that perform the audits, such as TÜV, new jobs have been established in order to fulfil this new task.

One of the operators interviewed does not fear negative headlines due to the obligation to report at all, since all systems are state of the art and that the authorities, as well as clients or other potential parties affected by an incident or simply a shortage in supply, would be notified anyway. On the other hand, it was also reported that the reporting obligation is likely to lead to negative headlines about the company reporting the incident. This then leads to companies being afraid and therefore less likely to make voluntary reports. In any event, negative headlines would be counterproductive and weaken the cooperation.

There are various improvements expected to be caused by the NIS law. Because companies are now legally obliged to deal with cyber-security for the first, the issue is no longer just an economic but also a social and state-regulated issue. This is hoped to be followed by a cascade effect, in the sense that also smaller companies, which are not subject to the NIS, recognise the necessity to deal with cyber-security. Furthermore, the NIS duty messages are expected to strengthen the exchange of information between the economy, computer emergency response teams, and the authorities again, because of this legal basis which now exists. Companies also

reported the benefits of process optimisation and harmonisation, sensitisation and enhanced awareness of employees, better collaboration as well as uncomplicated and fast exchange of information in the event of threats affecting cyber-security in order to be able to react quickly and appropriately.

Regarding additional financial burdens for the firms that are subject to the NIS, it was reported that additional financial expenditures and efforts that must be taken to prepare for the audits are substantial and should be subsidised.

There was only a rare number of precautious measures for the implementation of the NIS law because most systems had already been installed and data handled diligently regardless of the NIS.

5.6 Personal opinions:

Which further steps should be taken by the EU?

Goluch	- amend, improve, strengthen and make the NIS-Directive stricter in the next few years - assume that either more sectors will be included or that certain requirements for the safety measures will be given by the EU or that for example the threshold values will be clearly defined - would be a good idea to harmonise this after a few years
Gwehenberger	- at the moment - danger: fragmentation in the field of cyber-security: issue of cyber-security is being regulated in parallel in several areas. This naturally entails the risk that companies could be subject to multiple obligations. - but I hope that the EU, and in particular the Commission, will be aware of this and that progress will be made towards adequate harmonisation in this area. - It is also the case that the NIS Directive will be evaluated after five years.

Table 25: Further steps for the EU

Do you support the EU's approach to regulate security, especially cyber-security, by law?

Graf	- as far as the obligation to report is concerned, there will probably be no situation picture without the law. So, I understand the national interest here. - As far as safety precautions are concerned, especially the obligatory proof by other new qualified bodies and future audits, I think that companies can be burdened very considerably. - What the final outcome will be depends on what the catalogue of inspections looks like. That remains to be seen.
Plessl	- Of course, definitely yes. - Together we will strengthen each other and I think it is only possible with a regulation like this. - In principle, it is always to be questioned. I mean, you can also overregulate - no question. - But with regard to this cybersecurity, that is absolutely to be advocated, yes.
Anonymous	- Insofar as I didn't see it, I saw it done by our authority, the Austrian authority, with regard to critical strategic infrastructure. - We really were on an equal footing in terms of communication and the exchange of information, and we do not need legislation. That is the point behind it. It may not harm, yes, but it is not necessary. - The question is whether it is not too much effort, yes. We are only talking about IT systems now, yes. That's next, yes. I don't think so. I don't approve of that. - It's the same without the law.
Maier-de Kruijff	- Yes, because there are probably many organizations that would not take cyber-security seriously without laws. Especially small companies tend to assume that they are not in danger of an attack, because of their size, which is not true. - Another point is that only through harmonized regulation in the EU, can we generate a uniform level of security.

Table 26: Approach to regulate cyber-security

The opinions of the operators and the advocacy group are very diverse. On the one hand, the question, whether the NIS law or similar regulations are necessary at all, remains. In addition, the eventuality of financial burdens arising is a concern to some of the operators. On the other hand, however, many organisations were stated to bother with the whole topic of cyber-security for the first time due to the implementation of the NIS and can therefore also experience the positive effects of increased data security. Moreover, increases in transparency across the EU as well as offering the possibility to learn from other states' behaviour are also positive side effects.

Does the NIS law meet your expectations? (If not, where does it deviate?)

Goluch	- Overall, it meets my expectations in terms of what it ought to do: - does not regulate the cyber-security of the entire state of Austria - focused on certain areas, famous seven sectors - and there on focused on these essential services
Gwehenberger	- based on the so-called directive of the European Union - its present configuration is a compromise solution
Graf	- hope for good communication in both directions - As far as timely information in case of cyber-security incidents is concerned, this can be very positive because with good communication, we can fend off and eliminate incidents more quickly. - can also be very beneficial for the company
Plessl	- Of course.
Anonymous	- the advantage is of course, it is very transparent - already comprehensible - as a law it is definitely what I expect from a law. - …relatively clear. It is clear in principle which companies are covered and which are not. - definitely fulfils its purpose
Maier-de Kruijff	- Yes, in my opinion points such as the reporting obligation are positive because companies can benefit from it and a chain reaction of attacks can be avoided. - A uniform level of security in Austria and throughout the EU is also very good.

Table 27: Expectations

Conclusion on questions regarding personal opinions

The authorities interviewed hope and expect that the EU will further amend, improve and make the NIS-Directive stricter. It is assumed that more sectors will be included, threshold values will get clearly defined in order to harmonise the picture across the EU.

The interviewees' opinions towards the EU's approach to regulate cyber-security vary considerably. On the on hand, two of them heavily support this concept in order to create better awareness and get to advanced and uniform levels of cyber-security across all member states of the European Union. On the other hand, the operators

interviewed doubt the necessity of such a law meaning that things might be overregulated and therefore also overcomplicated. In addition, the financial burdens caused by the NIS regulation are of concern to the firms. However, the NIS law definitely meets the expectations very well, in terms of what it ought to do, i.e. it does not regulate cyber-security as a whole but is focused on the seven sectors and the essential services. The law was stated to be clear, comprehensive and transparent. Moreover, all parties can benefit and avoid many incidents as long as cooperation goes well.

5.7 Literature Comparison

Generally speaking, the feedback received in the interviews matches the literature well. The following paragraphs will point out the answers received in the interviews that contribute well to the existing body of literature. Furthermore, the answers given add valuable information to the research questions.

5.7.1 Matching Findings in literature

Member states show different degrees of difficulty regarding the successful transposition of EU directives due to divergences in their national laws (European Commission, 2018c). Thus, national laws must be adapted which might take some time and entail some infringement procedures by the European Commission. elaboration towards these goals, respecting their national laws, are up to the individual member states. Each member country is obliged to incorporate directives set by the EU into its national legislation (European Union, 2019).

In chapter *5.1* it was asked whether the implementation of the NIS law happened in time as well as whether the interviewees are satisfied with the proceedings. The answers met the expectations showing different degrees in the transposition. Although the transposition in Austria did not happen in time, as stated by the Ministry of Interior and by the operators of essential services, the implementation was successfully done, and all other goals were met. Moreover, the majority of the interviewees reported positively and mentioned the good public-private partnership. As already pointed out, some of the participants stated the law-making process was done rather quietly and therefore not fully transparent, it has to be mentioned that the NIS law is in itself a topic which is not meant to be communicated to a broad mass of addressees.

Our society is strongly dependent on a well-functioning infrastructure. However, maintenance of these vital functions is crucial for today's society, which forces security operators of essential services to take ongoing investments into their security

(European Commission, 2018a). Nevertheless, the insurance of security and cybersecurity is not only a major challenge for companies but also for the state, for the economy and the society not only in a national as well as in a cross-border context (European Commission, 2018a).

Cybersecurity is granted more attention than ever before, among policymakers, the industry, academics, the public and therefore in our everyday headlines. Since adversaries have become more determined, sophisticated and more likely to be connected to a nation state, cyberattacks have also occurred more frequent, sophisticated and threatening. Hence, growing insecurity concerning the privacy of data has grown. (Kuner et al. 2017).

Referring to chapter 5.2, two questions regarding sanctions displayed that sanctions are not a topic companies are particularly afraid of. Thus, at least the financial aspect of the NIS law is not a driver for rising insecurity. The operators interviewed by the researcher reported to have their systems up-to-date and handle their own as well as their clients' data with great caution and are therefore well protected against cyber threats. Nevertheless, no company is completely immune to attacks, which is why systems are upgraded and employees trained and educated consistently.

Since companies are now forced to fulfil these minimum-security standards audited once every three years, the NIS law is a subject, which is either about to cause increased effort, monetary expenses or support for companies in their attempt to strengthen Cybersecurity (Asllani, Ettkin & White, 2013). Nevertheless, such a law will permanently be highly controversial because there will always be a gap between personal rights, patents and copyright on one hand and the fight against cybercrime on the other hand. According to Asllani, Ettkin & White (2013, p.12) "cybersecurity should be considered a public good provided by the government."

Thus, security awareness is the crucial factor for the protection of not only organisation's but also human values. According to the infamous ex-hacker Kevin Mitnick, "Human Firewalls are a must!" (as cited in Helisch & Pokoyski, 2009, p5). This

implies that information security needs to take place in people´s consciousness, not in technology.

Bringing up chapter 5.3, minimum security standards, the results of this research stand in contrary to the literature. While the literature states that the NIS law will cause increased effort and monetary expenses, the interviews revealed this is as much as true as cybersecurity is a must. The minimum-security standards established are based on the European guidelines, whereas the threshold values were defined in cooperation with the operators of essential services. Nevertheless, it has to be mentioned that some companies are still concerned about potential financial burdens that might come along with their adherence to the NIS law.

*One of the main **reasons an incident reporting system** has entered into force is stated to be the **non-existence of such a regulatory system** in the whole European Union before (Nagyfejeo, 2018). Telecom providers formed the only exception being the only entities who already had to report their incidents before. Therefore, the NIS Directive was the ideal instrument to set up a strong regulation covering various cyber cultures (Nagyfejeo, 2018).*

*Since **cyber-security incidents are unhindered by national borders** and as history shows, numerous incidents were indeed not limited to single countries, it is absolutely necessary for all member states to act on common principles (ENISA, 2018a).*

*Many **advantages** go along with **effective incident reporting**:*

- *Fast distribution of information to all participants*
- *Coordination of responses and potential inclusion of different members input*
- *Access to expertise over the whole EU, not limited to single nations*
- *Identification and enhancement of good and best practices and dissemination of impractical or useless methods*

ENISA, 2018a

Looking back to chapter 5.4, all answers match the literature found. Except for some statements received by the operators claiming that the NIS law may be a cause for unnecessary effort, the interviewees agreed on the necessity of the obligation to

report. It was also stated the NIS law is a milestone for cyber-security, providing good standards and increasing resilience. Particularly striking, authorities and operators of essential services were of the same opinion that reporting would lead to better transparency and a better overview of the according situation. Moreover, the NIS law is expected to serve as a paragon for smaller enterprises, which are not addressed by the NIS, to endeavour enhanced cyber-security.

5.7.2 Limitations

The first limitation which has to be emphasised again, is the time factor. The NIS law is a very new topic and the implementation process is still ongoing. Consequently, none of the parties involved is able to report great experience yet.

Even though the researcher managed to have a representative cross-section of participants, including the authorities and operators of critical infrastructure from different sectors, it was not possible to receive any feedback from the Computer Emergency Response Teams. In addition, digital service providers could not be consulted either, since they do not receive a decree but have to identify themselves, as further elucidated previously.

5.7.3 Recommendation for further research

Since the NIS law was introduced rather recently and operators of critical infrastructure are still within the implementation phase, the change processes operators of essential services will be confronted with will be of concern in a few years, once the implementation process is finished and audits have taken place.

Hence, the researcher is convinced to be able to detect and verify that this respective law will have led to several change processes in two years from now within the context of a follow up master thesis. The query on whether these impacts are only relevant in an economic context or even for society as a whole will be part of the research. Furthermore, reflecting on the question whether changes in security will also have

been induced by this change management process after the implementation of the NIS law. Since the NIS law is expected to serve as an example for smaller firms, it would definitely be interesting to make out all the details and maybe find out that for some companies the law-making process was the start of digital transformation. Moreover, the researcher would like to identify the roots of the investigated companies' concern for cybersecurity and maybe even detect that the NIS law was the cause for some to deal with this topic in a serious manner.

Furthermore, the recent outbreak of the Corona Virus and the shutdown and economic crisis resulting from it, may cause some issues regarding data protection and cybersecurity, since decisions and operations now have to be taken very fast. Many firms were forced to implement new measures quickly in response to these special circumstances. Within the phase of a crisis, changes in the organisation of businesses have to be made and adaptations have to be done particularly quickly in order to be able to keep a business running. To name an example, possibilities to work from home, including many people being reliant on using their private notebook without proper security protection mechanisms, had to be opened. Despite everybody being reliant on a proper structure, data security may well be harmed due to the reduced diligence of employees resulting from this lack of time. All the issues resulting from the Corona Crisis, which have already come up or will potentially arise in the future, not only for businesses and the economy, but also for our society as a whole, would be of great significance for future research. Whatever sort of mistakes happen during such a crisis as well as their implications on the society and our everyday lives may well be an important indicator for the need to protect essential services.

6 Conclusion

Cyber security and legal regulations are always a controversial topic. The objective of this study was to investigate the economic and organizational impacts of the NIS law[2] on Austrian operators of essential services.

This is a descriptive, analytical study using the qualitative method of interviews on the one hand and members of the authorities, on the other hand members of operators of essential services as well as an advocacy group.

It can be concluded that the NIS law can definitely be seen as a milestone for security standards. For the first time, enterprises do not only apply internal, grown security standards or resort to existing standards ad libitum, but are legally obliged to fulfil the minimum-security standards and report serious incidents.
The main findings of this study are that the NIS is definitely a good starting point to increase transparency, create better awareness and get to advanced and uniform levels of cyber-security across all member states of the European Union. Furthermore, exchange of information between the economy, computer emergency response teams, and the authorities is expected to be enhanced. Companies also expect a variety of benefits from this law, such as process optimisation and harmonisation, sensitisation and enhanced awareness of employees, better collaboration as well as uncomplicated and fast exchange of information in the event of threats affecting cyber-security in order to be able to react quickly and appropriately.
However, while the elaboration process of the NIS law was fulfilled in a highly desirable manner, involving the economy and thus taking all relevant opinions into consideration, the question on whether it will actually be implemented successfully is still open. Furthermore, the actual necessity of such a law is doubted by some operators because of potential overregulation and overcomplication and therefore unjustifiable efforts for affected companies. Despite the authorities enthusiasm about the NIS law, they are also well aware of the fact that the law is not yet perfect and therefore expected to experience further adjustments, aggravations and improvements.

[2] Austrian Law according to the European NIS Directive

Resuming, it can be stated that the good partnership with the authorities will ease the fulfilment of all requirements for operators of essential services set by the NIS law. However, humans being responsible for the installation, maintenance, adaptation and monitoring of systems, will never be immune to make mistakes. Consequently, incidents can and always will happen, which is why the researcher's hypothesis can neither be falsified nor confirmed.

References

Allen, D., Karanasios, S. & Norman, A. (2014). Information sharing and interoperability: The case of major incident management. *European Journal of Information Systems*, 23, (4), 418–432. http://10.1057/ejis.2013.8

Almeida, R. A., Dickinson, J., Maybery, M. T., Badcock, J. C., & Badcock, D. R. (2010). Visual search performance in the autism spectrum ii: The radial frequency search task with additional segmentation cues. *Neuropsychologia, 48*(14), 4117-4124. http://dx.doi.org/10.1016/j.neuropsychologia.2010.10.009

Asllani, A., Ettkin, L., & White, C. (2013). Viewing Cybersecurity as a public good: The role of governments, businesses and individuals. *Journal of legal, ethical and regulatory issues, 16*(1), 7-15. https://www.researchgate.net/publication/289342389_Viewing_cybersecurity_as_a_public_good_The_role_of_governments_businesses_and_individuals

Boin, A., Ekengren, M., & Rhinard, M. (2015). *The Study of Crisis Management*. In V Mauer (eds), *The Routledge Handbook of Security Studies*. Abingdon-on-Thames: Routledge, 452–463

BSI. (2017). *BSI IT-Grundschutz-Standards*. Retrieved from https://www.onlinesicherheit.gv.at/experteninformation/normen_und_standards/bsi_it-grundschutz-standards/249143.html

BSI – KRITIS (2019). *Kritische Infrastrukturen.* Retrieved from https://www.bsi.bund.de/DE/Themen/KRITIS/kritis_node.html

Bundeskanzleramt. (2019). *Erläuterungen zum NIS-Gesetz*. Retrieved from https://www.bundeskanzleramt.gv.at/en/topics/security-policy/cybersecurity.html https://www.nis.gv.at/

Bundeskanzleramt. (2014). *Cybersecurity Report*. Retrieved from https://www.bundeskanzleramt.gv.at/en/topics/security-policy/cybersecurity.html

Cert.at. (2019). *Computer Emergency Response Team.* Retrieved from https://www.cert.at/index_en.html

Cert.at. (2017). *NIS-Richtlinie: Umsetzung aus österreichischer Sicht*. Retrieved from https://www.cert.at/reports/report_2016_chap04/content.html

Citizens Information. (2019). *Main aims of the European Union*. Retrieved from https://www.citizensinformation.ie/en/government_in_ireland/european_government/european_union/european_union.html

Clark, R., & Hakim, S. (2017). *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level (English Edition)*. Wiesbaden: Springer.

EASA. (2017). *What is CERT-EU, what is its role?.* Retrieved from https://www.easa.europa.eu/faq/24266

ECS. (2019). *Digitaleurope*. Retrieved from https://www.digitaleurope.org/resources/nis-implementation-tracker/

ENISA. (2019). *NIS Directive*. Retrieved from https://www.enisa.europa.eu/topics/NIS Directive

ENISA (2019a). *About Enisa.* Retrieved from https://www.enisa.europa.eu/about-enisa

ENISA. (2018). Minimum-security Requirements. Retrieved from https://www.enisa.europa.eu/topics/incident-reporting/for-telcos/guidelines/technical-guideline-on-minimum-security-measures

ENISA. (2018a). Good Practice Guide on Incident Reporting. Retrieved from https://www.enisa.europa.eu/topics/incident-reporting/for-telcos/guidelines/good-practice-guide-on-incident-reporting/good-practice-guide-on-incident-reporting

ENISA. (2017). Mapping of OES Security Requirements to Specific Sectors. Retrieved from https://www.enisa.europa.eu/topics/mapping/of/security/requirements

Europa EURLex . (2019). *EUR-Lex content statistics.* Retrieved from https://eur-lex.europa.eu/statistics/2019/eu-law-statistics.html?locale=en

European Commission. (2019). *Vertragsverletzungsverfahren*. Retrieved from https://ec.europa.eu/info/law/law-making-process/applying-eu-law/infringement-procedure_de

European Commission. (2019a). *Building strong cybersecurity in the European Union: resilience, deterence, defence.* Retrieved from https://ec.europa.eu/digital-single-market/en/news/building-strong-cybersecurity-european-union-resilience-deterence-defence

European Commission. (2019b). *NIS Cooperation Group's guidelines for implementing the NIS Directive and addressing wider cybersecurity policy issues.* Retrieved from https://ec.europa.eu/digital-single-market/en/news/latest-nis-cooperation-group-guidelines-for-implementing-NIS Directive

European Commission. (2018b). *State-of-play of the transposition of the NIS Directive*. Retrieved from https://ec.europa.eu/digital-single-market/en/state-play-transposition-NIS Directive

European Commission. (2018c). *2018 Commission report and factsheets on monitoring the application of EU law*. Retrieved from https://ec.europa.eu/info/publications/2018-commission-report-and-factsheets-monitoring-application-eu-law_en

European Commission. (2013). *Cybersecurity Strategy of the European Union*. Retrieved from http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%206225%202013%20INIT

European Commission. (2013a). *Critical infrastructure*. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

European Commission. (2013b). Cybersicherheitsplan der EU für ein offenes, freies und chancenreiches Internet. Retrieved from https://europa.eu/rapid/press-release_IP-13-94_de.htm

European Commission. (2013c). *Terrorism & other Security-related Risks (CIPS).* Retrieved from https://ec.europa.eu/home-affairs/financing/fundings/security-and-safeguarding-liberties/terrorism-and-other-risks_en

Europäische Union. (2019). *Österreich*. Retrieved from https://europa.eu/european-union/about-eu/countries/member-countries/austria_de

European Union. (2019). Regulations, Directives and other acts. Retrieved from https://europa.eu/european-union/eu-law/legal-acts_en

European Union. (2018). *EU institutions and bodies in brief*. Retrieved from https://europa.eu/european-union/about-eu/institutions-bodies_en

European Union. (2013). *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013PC0048

Gwehenberger, E. Ministry of Interior. (2019). Email

Hathaway, M. (2014). *Best Practices in Computer Network Defense: Incident Detection and Response.* Amsterdam: IOS Press.

Helisch, M, & Pokoyski, D. (2009). *Security Awareness Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung* 1st ed. Wiesbaden: Vieweg+Teubner.

Kaspersky. (2017). *What is Cybersecurity?.* Retrieved from https://www.kaspersky.com/resource-center/definitions/what-is-cybersecurity

Kersten, H., Reuter, J. & Schröder, K. (2016). *IT-Sicherheitsmanagement nach der neuen ISO 27001*. Wiesbaden: Springer.

Klipper, S., (2015). *Information Security Risk Management Risikomanagement mit ISO/IEC 27001, 27005 und 31010*. Wiesbaden: Springer.

KRITIS. (2017). Sectors of critical infrastructure. Retrieved from: https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sektoren_node.html

Kuratorium Sicheres Österreich. (2018). *Eigenes Gesetz für Cybersicherheitstandards bei Unternehmen.* Retrieved from https://futurezone.at/netzpolitik/eigenes-gesetz-fuer-cybersicherheitstandards-bei-unternehmen/400414118

Maglaras, L., Drivas. G., Noou, K. & Rallis, S. (2018). 'NIS Directive: The case of Greece', *EAI Transactions on Security and Safety*, 4(3), doi:10.4108/eai.15-5-2018.154769

Müller, K. (2014). IT-Sicherheit mit System. 5th ed. Wiesbaden: Springer Vieweg, pp.22-27.

Nagyfejeo, .E. (2018). EU's Emerging Strategic Cyber Culture(s). *Policing: A Journal of Policy and Practice, Volume Advance Article,* 0(0),1-24, Retrieved from: https://www.deepdyve.com/lp/oxford-university-press/eu-s-emerging-strategic-cyber-culture-s-vGKZYgTKA2?articleList=%2Fsearch%3Fquery%3Dincident%2Bmanagement%2Benisa%26dateFrom%3D2016-09-15%26dateTo%3D2019-09-15

Ranzijn, R., McConnochie, K., & Nolan, W. (2009). *Psychology and indigenous Australians: Foundations of cultural competence.* South Yarra, In Hallinan, M. T. (Ed.). (2006). *Handbook of the sociology of education.* New York: Springer.

Safa, N., Von Solms, R. & Furnell, S. (2015). 'Information security policy compliance model in organizations', *Computers & Security*, 56, 70–82, doi: 10.1016/j.cose.2015.10.006

Schallbruch,M. (2017). *The EU Directive on Network and Information Security: Requirements for Digital Services.* Retrieved from https://knowledge.esmt.org/article/eu-directive-network-and-information-security-requirements-digital-services

SchengenVisaInfo. (2019). *The European Union and Countries in the EU*. Retrieved from https://www.schengenvisainfo.com/eu-countries/

Theiss, W. (2016). *MANDATORY EU CYBERSECURITY STANDARDS IN CRITICAL BUSINESS SECTORS AND IN DIGITAL SERVICES*:. Retrieved from https://www.wolftheiss.com/fileadmin/content/6_news/clientAlerts/2016/2016_Q3/160906_WT_CA_Mandatory_EU_Cybersecurity_standards.pdf

Vahs, D. (2009). *Organisation*. Stuttgart: Sage Publications Ltd.

Sources of Law

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. [Online]. [Accessed 26 March 2019]. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505297631636&uri=COM:2017:476:FIN

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. [Online]. [Accessed 26 March 2019]. Retrieved from https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Directive (EU) Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). [Online]. [Accessed 26 September 2019]. Retrieved from https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32002L0021

NISG - Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) BGBl. I Nr. 111/2018. Fassung vom 29.12.2018. [Online]. [Accessed 26 March 2019]. Retrieved from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536

NISV - Verordnung des Bundesministers für EU, Kunst, Kultur und Medien zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssystemsicherheitsverordnung – NISV) BGBl. I Nr. 215/2019. Fassung vom 28.8.2019. [Online]. [Accessed 28 August 2019]. Retrieved from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010722

Methodology

Agee, J. (2009). The interview reconsidered: context, genre, reflexivity and interpretation in sociological approaches to interviews in higher education research. *Higher Education Research & Development*, 32, (1), 5–16, doi: 10.1080/07294360.2012.750277

Bogner, A., Littig, B., & Menz, W. (2009). *Interviewing Experts*. Wiesbaden: Springer.

Braun, V. & Clarke, V. (2012). Thematic analysis. In H. Cooper, P. M. Camic, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (Eds), *APA handbook of research methods in psychology, Vol. 2: Research designs: Quantitative, qualitative, neuropsychological, and biological*. Washington, DC: American Psychological Association, 57-71

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*, Thousand Oaks: Sage.

Clegg, S. & Stevenson, J. (2013). Developing qualitative research questions: a reflective process. *International Journal of Qualitative Studies in Education*, 22, (4), 431–447, doi: 10.1080/09518390902736512

Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches.* Thousand Oaks, CA: Sage Publications.

Deterding, N & Waters, M. (2018). *Flexible Coding of In-depth Interviews.* Sociological Methods & Research, 1, doi: 10.1177/0049124118799377

Duncan, N. J. & Hutchinson, T. (2012). 'Defining and describing what we do: Doctrinal legal research', *Deakin Law Review*, 17(1), 83–119, Retrieved from http://openaccess.city.ac.uk/4335/

Flick, U. (2014). *An Introduction to Qualitative Research*. London: Sage Publications Ltd.

Gill, P., Stewart, K., Treasure, E. & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups BDJ. 204, 291–295, doi: 10.1038/bdj.2008.192

Josselson, R. (2013). *Interviewing for Qualitative Inquiry: A Relational Approach*. New York: Guilford Publications.

Opdenakker, R. (2006). 'Advantages and Disadvantages of Four Interview Techniques in Qualitative Research', *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 7*(4), doi: 10.17169/fqs-7.4.175

Tyler, T.R., (2017). 'Methodology in Legal Research', *Utrecht Law Review*, 13(3), 130–141. doi: 10.18352/ulr.410

7 Appendix 1 Interview Goluch

Larissa: Within the scope of my Bachelor thesis, I will now conduct the following interview.
Do you agree on the publication of this interview and your name?

Gernot: Yes.

Then I would ask you to introduce yourself and to quickly describe the organisation you work for as well as your area of responsibility.

Gernot: Sure. My name is Gernot Goluch. I am the head of the division 5.3 in the BVT (Bundesministerium für Verfassungsschutz und Terrorismusbekämpfung – Ministry for constitution protection and counterterrorism). That is the NIS division in the department cybersecurity. Everything concerning the NIS law is concentrated here, i.e. everything regarding the operative implementation of the law; audits and reports received. All these things happen here in the department 5.3. On the other hand, there exists the strategic NIS administration in the Federal Chancellery. This is our counterpart who deals with strategic matters, such as possible amendments, which would for example identify operators of essential services. This is what the European initiatives do. Yes, this is my task area in the department 5.3.

Larissa: So what exactly was your area of responsibility regarding the NIS law?

Gernot: I am not a jurist. I was actually coming from the subject-specific section of IT-security, information security and my major duty there was to provide technical input, e.g. which safety measures are demanded from the operators or how processes are audited. In addition, i was involved in discussions concerning infrastructure, sectors and with CERTs or other ressorts, i.e. all departments concerned with the NIS. My colleague, Erik Gwehenberger, who who will be interviewed later on I think, has done all the legal activities of the BVT Division 5. This means to read through all acts and to integrate the qualified entities regulation into the regulatory. He has done these legal activities. The technical input came from me, as well a lot of communication in advance with all addressees of the NIS law.

Larissa: What was the implementation of the NIS law from the authorities' point of view like?

Gernot: I have to say that this was my first time being part in a legislative process. I would say very positive because all parties involved cooperated very well. We tried to meet representatives from every sector in I think three discussion rounds in order to find out what makes sense and what does not. These are things such as incident reporting thresholds – when is a security incident to be classified as highly critical, for instance in the sector health care. We experienced very good and strong cooperation between the economy and the authorities, on the one hand the Inner Ministry, but also the Federal Chancellery. All in all, my experienced was very positive. Within the process of commenting on the law we received a lot of statements, which were all read through, especially by my colleague Erik Gwehenberger, but also by the colleagues in the Chancellery. They were also partially incorporated into the final legal text. I would almost say all the proceedings with the involvement of the addressees was exemplary. I experienced that very positive. The small downside, of course, is that if you involve a lot of people, a lot of people know about the status of the law or the law in itself and, of course, get slightly impatient. But I think that this small negative connotation, which is definitely outweighed by the positive of the cooperation. So there was little resistance, for example.

Larissa: Does the NIS law meet your expectations or do you see any deviations?

Gernot: No, so I would say, overall it meets my expectations in terms of what it ought to do. What do I mean by that? The NIS law does not regulate the cyber security of the entire state of Austria. It does not. That was never the idea. But it is very focused on certain areas, namely on certain sectors, these famous seven sectors, which are mentioned in the law and there on focused on these essential services. The NIS law does not care about any privacy concerns, for example. This is what data protection laws are for.

Larissa: Such as the GDPR.

Gernot: Exactly. The NIS law is only concerned with operators of essential services who are operators of big critical infrastructure, and not with the cyber security of

medium-sized companies. However, looking at the big picture, I feel like the NIS law is a very good law, well implemented and meeting my expectations. But, as I already mentioned in various discussions and presentations, it is a first important step in the right direction concerning cyber security, but it is not the end yet. This is my personal opinion.

Larissa: Could the implementation into national law be realized as planned, i.e. the of the transposition directive into the NIS law.

Gernot: Yes, if you ignore the temporal component, yes. In terms of time it is true that Austria was already in arrears along with many other member states. It would be 2016, I think…

Larissa: The directive was issued in 2016.

Gernot: Exactly. Actually it should have been implemented in 2018, namely in May 2018 but was fully transposed at end of December 2018. Since then, there have been inquiries from the Commission, why there is nothing going on but in 2018, a few months late, it was then implemented. However, there are other European Member States, which did even later. That does not make Austria any better now in the sense that we were better, but delays occurred in some Member States.

Larissa: Do you know if until now that has been implemented by all states?

Gernot: As far as I know, yes indeed. But I do not know if there are laws regarding the operative transposition of the directive in other EU countries.

Larissa: Was goldplating done or the target overshot?

Gernot: No, not in Austria. We have adopted exactly the sectors of the EU directive. The only thing that has happened in Austria is that the public administration has also committed to stick to the law. The state says “I have to obey the law myself, if I ask of the critical infrastructures to do so.” Certainly, that makes sense. It's exactly the seven sectors mentioned in the NIS. I believe it will, for example, will be a point of discussion for the future, if other sectors should be integrated in a few years that are not within the scope of application now. But that is only my professional opinion - whether that is then politically, legally implemented, I do not know.

Larissa: Which sectors can you imagine to be included?

Gernot: Let's take the simplest example, which is also noticeable through various comments already published by different people. It is for example drinking water is present, but not wastewater. That actually does not make much sense from a purely logical point of view, since in Austria in particular the drinking water sector is, as they say, very physical. Vienna for example high spring water pipe flows in and that flows simply by physics. There is relatively little digitization here. However, looking at sewage, there are sewage treatment plants, which of course is very heavily digitized. That does not really make much sense from the pure critical infrastructure perspective of not including wastewater but drinking water. That's just the result of the directive. These are national specifics. That's okay as a first step but I imagine there could be changes in both EU and national terms over the next few years. But this is just me guessing. I do not know anything more. We also hear that they want to be innovative at European level, in the sense that they want to revise the directive and include more sectors. Thus, there's something else that can happen in Europe too. But that is all in the big cloud of EU bodies. I do not have any idea about the status right now.

Larissa: What improvements can be expected from the NIS law?

Gernot: They are almost obvious. In my opinion two main improvements can be expected. I need to open up a little more the scope for the first one; Information security has actually been a private issue in many areas. Of course, there are legal regulations such as data protection law and so on and so forth, have the inside, only if a company now a certain amount of risk to take in terms of information-cyber security – it was an economic decision at the end of the day. Now these economies must be integrated according to the law. Thus, it is now no longer purely an economic issue but a social issue, a state-regulated issue. I assume, that the information, IT, cyber security, whatever you want to call it, increases or, at least, will be unified in some sectors. IT companies, for example, in some sectors, it is not very great in terms of security so far and some might actually do great, but they are adjusting. However, I think that the whole security area will experience a boost, simple due to the regulatory act. There is now even a law which requires companies to implement certain security measures. Such a thing did not exist before. The first big factor and a second improvement that I think I will come, is NIS duty messages that will strengthen

the exchange between economy, computer emergency response teams, authorities simply again, because it is now a legal basis exists.

Larissa: Do you think that all of these things are factors, of which the population can in some way perhaps feel more secure, or is that all something that actually takes place sort of behind-closed doors

Gernot: Realistically, the population will not feel any impacts of the NIS. However, you have to say that security is always an issue. You will not notice safety and security only if it is no longer present. Security in a positive sense is often hard to come by. Now, if, theoretically, critical infrastructure broke done somewhere because cyber-security measures had been dismissed, then it is to be noted by the population, but we hope to avoid that through the law. As long as the law works well and incidents are properly reacted to, only the NIS' addressees of its obligations will know about it. Thus, the broad mass of people will not feel know about it as long as everything works and will likely not report to feel much safer. This will take place at the level of the economy, the authorities and the cyber security community.

Larissa: If you think back to the development process of the law, how do you feel about the cooperation between the state and the economy?

Gernot: I mentioned it in the beginning – very positive. All interest groups, individual companies, or representatives of the authorities communicated at the same level. Years ago, some colleagues from another Department have already started with the conduction of sector meetings where all parties involved where invited and where we explained the rules and how they should be implemented. I think you can see it even now in the ongoing cooperation; everything works well and there are little complications and negative headlines or bad vibes. On the other side, we are not trying to be the black hole of the authority. If anybody comes to us with questions and we will reply accordingly. There's a very lively exchange of ideas now. I say that as an example: I cannot think of any bad large-scale campaigns during the process of the creation of the law. Overall I have to say everything worked well - in terms of society, or any branch of the economy or whatever.

Larissa: How is the cooperation with the economy, in this case with the operators of essential services, assessed from the authorities' point of view?

Gernot: As I said, very good, very cooperative. Of course, it is about to be exciting now, when it comes to the operating doing. It will be exciting to be in maybe one, two, or three years from now in a situation when the audits are done and it is assessed which firms actually act according to the law. might need to ask one critical question first - why a message has not been refunded. So potential for conflict is still present. I don't see it as too big. One must also always bear in mind, these companies are now no companies, where the theme was alien. We have contacts in all these companies, so in the majority of the companies with whom we had contact, where there are people to whom the topic is very important. That is, we are viewed very often as a Partner, the authority is less than the cyber police, who prescribes something. Because the measures are there in the law, in the regulation, it must be explained to someone in the company that would be important to implement the. Often there is even a back, to communicate with whom, internally, because he says, "I want to do anyway, the law." The law calls for that too, and then maybe internally at the company and then also Budget get or so. We have one, two, three years once in a Situation where you may need to will then require but once what, or if you ask one critical question first: why a message has not been refunded. This has, of course, so the potential for conflict is present. I don't see it as too big. One must also always bear in mind, these companies are now no companies, where the theme was alien. We have contacts in all these companies, so in the majority of the companies with whom we had contact, where there are people to whom the topic is very important. That is, we are viewed very often as a Partner, the authority is less than the cyber police, who prescribes something. Because the measures are there in the law, in the regulation, it must be explained to someone in the company that would be important to implement the. Often there is even a back, to communicate with whom, internally, because he says, "I want to do anyway, the law." The law calls for that too, and then maybe internally at the company and then also Budget get or so.

Larissa: What measures were preliminarily taken with the economy involved?

Gernot: Measures in what sense?

Larissa: the cooperation in this sense.

Gernot: Measures in what sense?

Larissa: To prepare for the cooperation.

Gernot: Well, on the one hand we had the sectoral discussions and then - I think this is something that has to be emphasized again and again - the statements received from the economy on the part of the legislature have all been processed. There was not a single opinion that was not considered, and if you look at the law, before the opinion process as well as after it, really major changes were done there. Positive changes, reported by the business community, which were registered by the public.

Larissa: Why are qualified bodies established and what are their accreditation criteria?

Gernot: I will start with the first question: Why? There must be somebody who checks every three years if this company A actually implements all security measures. There are different models, also in Europe. One model would be for the authority itself to go and check on the spot what the operators of essential services are doing. This comes with two issues which are the reasons why we did not decide on doing that either, because of course, that would be an absolutely valid option. Why do we not do that? The first issue is very simple. We are talking about 100/150 operators of essential services, these are big companies. In Austria, we simply do not have the resources to intensively, even in a three-year cycle, constantly conduct audits. We simply do not have the people. And even if we had the posts for it, you first have to get the specialist staff to do it. This is a highly competitive market in Austria. That means people with many years of information experience, testing experience, technical, organisational experience that are hard to get are needed. That is the first problem, but well, let's assumed we solved that. The second is: these companies can already be audited anyway. There is no operator of essential services who does not do out audits now, at least principally speaking. Now there are companies in Austria who do that. They are already doing a good job and they are already being commissioned. Our idea was to basically appoint such companies if they meet the requirements as qualified bodies so they can immediately participate in the inspection according to the law in their inspection activity. This results in less burden for the

operators of essential services. There will be a bit more effort, but it will not be huge. On the other hand, they do not have to go through this procedure again and be again blocked for one or two weeks, because then BMI auditors will be permanently in the house, where perhaps three months before a private company has done an audit anyway. The important thing is: the qualified body checks, but we as the authority always verify and decide whether the check is really positive in the sense of the law. That means that I and my staff do that. In other words, the qualified body only determines what has been established, but we then approve it.

Larissa: And what are the criteria for accreditation?

Gernot: There is the qualified bodies regulation, I think the abbreviation is Quaste V or something like that where all the criteria are defined, e.g. they have to prove that they take care of their own information security, that the test data is stored securely, they have to prove centrally that they have a certain minimum number of examiners with a minimum of professional experience, and then they have to prove that these examiners have been involved in all these specific areas, because, after all, security measures, training, experience, testing activities, etc. In other words, they simply have to provide formal proof of what I am doing at the moment. These are the first candidates who have reported that they are really being examined: Can they meet all the conditions laid down in the regulation? If so, they will be appointed by notice to be allowed to check everything or certain measures.

Larissa: What criteria were used to select the minimum safety standards?

Gernot: They are very much attached to the European guidelines, so there are hundreds of standards that deal with cyber security. And the Commission, I think exactly, it was a NIS Working Group of the Commission has a paper which has just issued a paper in which these security measures were described and in principle we have taken these security measures and have written this into the regulation nationally. What we have already done is; and the description of the measures already came strongly from u, we didn't translate and adopt everything one-to-one, but rather looked through it, perhaps applying stricter standards here and there, a little. Maybe a little less strict here and there. Generally speaking, though, we have to say that the

Regulation is very generic in its description anyway. These are not detailed descriptions. In any case, sector-specific standards must be set.

Larissa: What criteria were used to define the thresholds?

Gernot: We had ideas and templates, what should adhere to. The thresholds, that was done by the Federal Chancellery, but we were strongly involved. In principle, we sat down with the operators and sectors and really thought it through together: what is a reasonable threshold value for sectors A, B, C, D and did the same also for sub-sectors. In other words, this was done together with the industry. Mostly it is the number of the population, so how many people are affected or the time factor. But that is really totally different. You can also read that in the NIS regulation. It is partly different for some sub-sectors, for some sectors completely different. Sometimes it is user hours, sometimes it is a pure time component, sometimes it is metering points in the electricity sector for example and so on.

Larissa: Are frequent sanctions to be feared?

Gernot: I don't think so. Why: First of all because these are big companies, which have to and want to take care of the topic in a positive way. This means that we are not talking about an area where we come across companies that have said up to now, "I don't care about this topic." Secondly, the fact is that we in Austria are going the official way anyway: first consultation and then punishment. This means that if, for example, a company sends in a mandatory report too late, the first step will not be to initiate criminal proceedings, because we want to cooperate well with the companies. This means that first of all we will sit down together and explain "this should have happened faster". Then you let this company explain the situation and only if this happens repeatedly, criminal proceedings would follow. Same thing is true for security. I think that most problems can be solved in good cooperation, but of course you have to be realistic when we talk about 100/150 companies, there will be sanctions at some point. This is the case with almost every law and they will probably be judged by the legal authorities and then there would be a decision. I expect this to be a rare and would be surprised if otherwise. So, I would be very much mistaken if a very large number of sanctions had to be imposed. This would actually only be an indicator that the cooperation in the area between the economy, the authorities and

society no longer functions well. It would be more of a warning signal that there is really something that must be improved.

Larissa: Otherwise, would there be any fear that the cooperation with the economy would be weakened by such sanctions?

Gernot: Yes, double-edged. If the cooperation was weakened for whatever reason, or if the cooperation would not work anymore, then this would inevitably lead to a higher number of sanctions, because there would no longer be a good basis to cooperate and in the end the penalty notice would be sent to the operator. That means I would turn it around. At first, there is the bad mood or bad cooperation, then the penalties follow. If we were to go to the other side and, as an authority, were to go out immediately with penalty notices before we communicate, before we talk to the operator, before we try to solve things in good cooperation, then cooperation would inevitably deteriorate and that would be very bad for the whole issue of cyber security. Because we would end up in an area where, for example, we would no longer receive any voluntary reports, where communications between the authorities and the business community would be reduced to the minimum legal requirements, and that would make the current situation worse. But if you are an authority that never issues sanctions, if you always say yes and amen to everything, and then at some point where you get the call "They're just waving everything through anyway", then that would hurt the cooperation, because then you wouldn't be taken seriously either. In other words, where it will be necessary to have follow-up consultation, follow-up cooperation, there will certainly have to be the possibility of sanctions, which we would then also implement - of course. But of course within a reasonable framework and always with this cooperation in mind. That is very important.

Larissa: In your opinion, does the obligation to report contribute to get a better picture of the situation?

Gernot: Exciting question. There are two. There is the mandatory reporting and there is the voluntary reporting. The compulsory report has to be done. The threshold values are very high. In other words, mandatory reporting is necessary if something really serious happens. That means if for instance electricity failed somewhere or ÖBB could not run any more trains through the area. So that's when the little man and

woman on the street notice it. I hope and assume that we will not get too many obligatory reports. That would be bad, because that would mean that we have a huge problem in this area. The voluntary registrations are much more important because I quote doctor Schwabl from the A1 who will explain it...how did he say? He will measure the success of the NIS law by the number of voluntary declarations. That is an exciting statement. So, the more voluntary reports we get, the more you cooperate, the more open you are, so also this Near Misses, so now something almost happened and I might report it anyway. If we manage to do that, then the situation will be much improved once again. If you...if this voluntary exchange of messages does not work, then you are dependent on the obligatory messages and hopefully there won't be many of them.

Larissa: Is it possible to strengthen the cooperation between state and economy or are there also negative influences of the NIS law?

Gernot: So far, I don't see any. But it is only now beginning to be operational. I believe that at the moment we definitely are on the right track, shaping the whole thing positively and there are always sensitivities here and there. There always will be, but I think that on the whole it works very well. There is always the danger that the mood could deteriorate for a variety of reasons, but I do not only believe what we are doing now in the context of the NIS Act, but the entire Department Five. When it comes to incidents, incident support for critical infrastructures, for other departments, along with computer emergency teams and so on. I believe that this is a good, fruitful cooperation at the moment, and we are increasingly perceived as a good and reliable partner. Everything is still within the stage of construction. But I believe that at the moment it is pointing in a positive direction. But of course, you have to be careful that it stays that way and keep working on it. That is not a question.

Larissa: So, you think that the reporting obligation will help to improve transparency?

Gernot: Yes, in the closed circle of the addressees. Because at the very moment a mandatory report is made - which of course we won't do - but let's say a company sends a mandatory report and five minutes later reads its own report in the newspaper. Then we would have a problem. But as long as this remains, so to speak, transparent within the circle of the sectoral, the CERT, that is to say the computer

emergency response team, authorities and operators, I believe that, firstly, we can certainly create more transparency and exchange of information, which is almost even more important. Of course, not everything must be made public now. Understandably, companies are also afraid of this to happen, because if every report of a problem was published four hours later in the Kronenzeitung, in the Standard or wherever, then we would of course have a problem.

Larissa: At the end: Which further steps should be taken by the EU?

Gernot: Well, all I know is, I heard someone from the Commission recently who said that they will have to amend, improve, strengthen and make the NIS directive stricter in the next few years anyway. So, I think I almost assume that either more sectors will be included or that certain requirements for the safety measures will be given by the EU or that for example the threshold values will be clearly defined. Because that is the way things are now: each EU state is doing its own thing. There are those who set the thresholds very high. In Germany, for example, they have now set it rather low. This creates a bit of a rag rug. It would be a good idea to harmonise this after a few years, now that the NIR Directive has been implemented.

Larissa: To get a uniform picture, I suppose.

Gernot: Right. Exactly. Let me give you an example: Let's say that we identified the biggest electricity operator in Austria, I don't know, any of the big ones. Which we haven't done, but only in theory. And in Slovenia they would have taken all the major ones above a certain lower threshold. You will find yourself in a situation where companies in one country are not covered by the NIS law and in the other country they would be covered in terms of size. And that doesn't really make sense, because the entire sectors are extremely dependent on each other... not all of them, but a lot of them, for example, the e-economy. So, if something major happens in Italy, it naturally affects Germany and so on and so on. In other words, there will certainly be harmonisation. What would be important is that the essential services link up the EU so far that I know the essential service in the neighbouring country does not matter now - in Germany depends on the essential service in Austria. That does not exist at the moment. But that would be extremely important, because if we knew that, then we could also increase the passing on of information. It could be that an essential

service in Finland depends on the essential service at Vienna Airport. That could be... and one more thing which is very important. That is NIS policy on the one hand. Surely there is still a lot to be done, harmonisation, linking essential services in the different EU member states and so on. Another thing has already been tackled anyway. I believe that the Cybersecurity Act has been implemented in March, because if you look at it, the NIS Directive is now very much aimed at the operators of essential services. They all have suppliers, for example. They buy products. Siemens, ABB and so on, whatever they're called. And, of course there is always the question: this product certification, this product safety - this is now to be regulated within the framework of the Cybersecurity Act. So my suggestion would be that we now look a few years into the future, that there should be a very clear scheme for product certification for industrial control technology, for example, and that the operators of essential services covered by the NIS Directive should then be required to buy such safe products. I believe that this would be another important step to take. But cybersecurity is a very big thing to work on in general. There is a lot in it, so it is not just this certification that is in it. It's also there. It's also about certifying products for the general public. That is for example when you buy a router at Media Markt. That there is no damage password or anything like that. There are some things. So, these are the big things that I would expect in Europe. Whether they will come, I don't know.

Larissa: Good. Thank you very much for your time.

Gernot: My pleasure. Thank you for the chocolate.

8 Appendix 2 Interview Graf

Interview Alexandra Graf Deutsch:

Larissa: Ähm für meine Bachelorarbeit zum Thema Auswirkungen des NIS Gesetzes auf österreichische Unternehmen wird das folgende Interview durchgeführt. Sind Sie damit einverstanden, dass dieses Interview aufgezeichnet und veröffentlicht wird?

Alexandra: Ja.

Larissa: Dürfen Angaben zu Ihrer Person veröffentlicht werden oder möchten Sie, dass dieses Interview anonymisiert wird?

Alexandra: Angaben zu meiner Person können veröffentlicht werden im Rahmen der Bachelorarbeit.

Larissa: In diesem Sinne würde ich Sie dann bitten, sich selbst einmal kurz vorzustellen, sowie auch die Organisation, in der Sie tätig sind und Ihren Aufgabenbereich in dieser kurz zu beschreiben.

Alexandra: Ja mein Name ist Alexandra Graf. Ich bin beschäftigt bei den Salzburger Landeskliniken. Die Salzburger Landeskliniken sind ein Gesundheitsdienstebetreiber. Das heißt, wir ah betreiben fünf Krankenhäuser, davon zwei Universitätskliniken. Äh wir haben etwas über 6000 ah Mitarbeiter und sind einer der wesentlichen Gesundheitsdiensteanbieter im Bundesland Salzburg. Ich bin der Chief Information Security Officer der Salzburger Landeskliniken, äh organisatorisch aufgehängt beim Geschäftsführer.

Larissa: Gut. Dann trägt die Meldepflicht Ihrer Meinung nach zum Gewinn eines besseren Lagebildes bei?

Alexandra: Ah aus Sicht der Behörden gehe ich auf alle Fälle davon aus, da ich glaube, dass sich die Unternehmen bisher eher zurückhaltend verhalten haben und eine Meldepflicht ja auch eine Pflicht ist und daher die Meldungen wahrscheinlich steigen werden.

Larissa: Naja, es könnten ja auch freiwillige Meldungen abgesetzt werden, in welchem Ausmaß das auch immer dann getan wird dann in der Praxis, aber ja. Kann Ihrer Meinung nach hiermit die Zusammenarbeit zwischen Staat und Wirtschaft gestärkt werden, oder sind für Sie negative Einflüsse des NIS Gesetzes merkbar?

Alexandra: Naja, das kommt jetzt darauf an; Grundsätzlich glaube ich schon, dass die Zusammenarbeit zwischen Staat und Wirtschaft gestärkt werden kann. Wie das dann konkret gelebt wird äh, ist natürlich abhängig davon, wie die Behörde jetzt damit auch umgehen wird. Ähm ich glaube, dass es noch wichtig sein wird, äh bei einem Sicherheitsvorfall ähm eine gute Vernetzung von den bundes- und landesweiten Verantwortlichen zu definieren und zu kommunizieren. Äh ich spreche jetzt beispielsweise vom Bereich des staatlichen Krisen- und Katastrophenmanagements, wo ja Kompetenzen auch in den Ländern liegen und das muss glaub ich auch noch gut vernetzt und abgestimmt werden, wer dann welchen Ball sozusagen hat.

Larissa: Wird die Meldepflicht trotzdem dazu beitragen, Transparenz zu verbessern?

Alexandra: Also aus Sicht der Behörden glaube ich auf alle Fälle, da mehr Meldungen eingehen werden und ähm was mich jetzt betrifft (husten) geht es jetzt nicht so um die Transparenz. Mir ist es wichtig, um eine Information wenn jetzt beispielsweise bei einem anderen Betreiber eines wesentlichen Dienstes ein Sicherheitsvorfall eintritt, weil so ein Vorfall ja auch auf unser Unternehmen Auswirkungen haben könnte und ich hoffe dann schon, dass bei einer guten Kommunikation zwischen den Playern, also zwischen den

Larissa: Betreibern.

Alexandra: genau, zwischen den CERTs und Betreibern Sicherheitsvorfälle dann auch schneller abgefertigt werden können.

Larissa: Wie ist bis jetzt die Kommunikation mit den Computer Notfallteams und mit den anderen äh Betreibern wesentlicher Dienste beziehungsweise kritischer Infrastrukturen?

Alexandra: Es gibt Kontakte zwischen beispielsweise den Betreibern wesentlicher Dienste, was jetzt meine Branche betrifft. Äh mit den CERTs…das CERT ist ja noch sehr jung. Da kann ich jetzt noch nicht von Erfahrungen sprechen.

Larissa: Okay. Befürchten Sie, dass es durch die Meldepflicht auch zu Negativschlagzeilen kommen könnte für Ihr Unternehmen?

Alexandra: Das hoffe ich nicht. Das wäre ja auch kontraproduktiv. Man wird sehen (lacht).

Larissa: Wenn Sie an den Entstehungsprozess des Gesetzes zurückdenken, wie beurteilen Sie die Zusammenarbeit zwischen Staat und Wirtschaft, also zwischen den Behörden und Ihnen?

Alexandra: Also ich war jetzt am Entstehungsprozess nicht wirklich beteiligt und kann dazu jetzt auch nicht wirklich etwas sagen.

Larissa: Wie ist die Umsetzung des NIS Gesetzes aus Ihrer Sicht bisher verlaufen?

Alexandra: Grundsätzlich gut. Ich nehme wahr, dass die Behörde sehr bestrebt ist, zu informieren. Die Behörde ist auch auf uns zugegangen in Form von Informationsveranstaltungen. Ähm interessant wird es jetzt, ähm was die konkreten Definitionen von wesentlichen Diensten und schlussendlich auch die der Sicherheitsvorkehrungen betrifft. Ich finde, da muss jetzt noch einiges abgestimmt werden, äh vor allem bedarf es eines spezifischen Branchen-Knowhows. Es ist beispielsweise bei einem Stromversorger einfacher festzustellen, ob ein Dienst verfügbar ist oder nicht. Also, das heißt, es gibt Strom oder es gibt keinen Strom. Das kann man klar definieren. Kann man auch gut nachweisen. Bei einem Krankhausbetreiber ist das wesentlich komplexer, weil zum Beispiel ein wesentlicher Dienst wie die Versorgung in einem Schockraum auch verfügbar ist, wenn ein IT-System nicht verfügbar ist und hier ist es wichtig, einen guten, gemeinsamen Weg mit der Behörde zu finden. Insbesondere muss der Prüfkatalog dann auch entsprechend das beinhalten und auch abgegrenzt werden.

Larissa: Wie war bisher die Zusammenarbeit mit den Behörden? Sie haben gesagt, sie ist bestrebt, Sie zu informieren – sonst auch alles positiv oder…?

Alexandra: Genau. Durchaus. Wir wurden immer wieder informiert. Wenn ich jetzt in die Zukunft schau äh, wird es interessant, wer jetzt qualifizierte Stelle sein wird und wie der Prüfkatalog aussieht. Ähm ich ähm würde es auch sehr begrüßen, wenn der Prüfkatalog nach bekannten Normen erfolgt, beispielsweise ISO27001 und dann der Scope von den qualifizierten Stellen dann klar abgegrenzt ist.

Larissa: Wurden Sie auch in die Sektorengespräche miteinbezogen?

Alexandra: Teilweise, ja.

Larissa: Welche Vorkehrungen wurden in Ihrer Organisation zur Umsetzung des NIS Gesetzes getroffen?

Alexandra: Also wir haben unabhängig davon auch ein Projekt gestartet, in dem unter anderem auch die Vorgaben des NIS einfließen werden.

Larissa: Wollen Sie das näher erläutern oder ist das noch zu jung?

Alexandra: Ich glaube, das würde den Rahmen jetzt sprengen.

Larissa: Okay. Gut. Kam es in der Organisation Ihres Unternehmens zu Veränderungen?

Alexandra: Also im Bezug jetzt auf das NIS Gesetz ähm in der Form, dass wir sobald wir den Bescheid haben ja auch eine Meldestelle nominieren und diese dann auch einrichten müssen. Die anderen Punkte wie klassisches ISMS, Zertifizierungen, und Katastrophenpläne,..bei uns heißt das OGK, Organisation für Großereignisse und Katastrophen. Diese Punkte waren schon auf unserer Agenda und sind am Laufen. Ähm Sie dürfen sich vorstellen, dass das Thema Informationssicherheit eins unser ureigenes Interesse ist. Das heißt, wir äh möchten alles Vertretbare und werden alles Vertretbare tun, um die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen sicherzustellen. Das ist ja unabhängig vom NIS Gesetz eines unserer ja ureigenste Interesse des Unternehmens.

Larissa: Das heißt, das NIS Gesetz war jetzt auch keine besonders große Hürde für Sie?

Alexandra: Naja, das wird man sehen, weil die große Unbekannte ist ja jetzt der Prüfkatalog und was wird alles geprüft – und ich hoffe, dass man sich schon an die herkömmlichen Nomen halten wird und vor allem den Scope – ich habe es vorher schon erwähnt – dass das bei einem Krankenhausbetreiber ja etwas schwieriger ist, als beispielsweise beim Energieversorger, dass man den ähm einfach zweckmäßig definiert.

Larissa: Also ist dadurch auch kein zusätzlicher finanzieller Aufwand entstanden oder irgendwelche neuen Arbeitsplätze geschaffen etc.?

Alexandra: Also Arbeitsplätze die konkret das Mascherl NIS Gesetz haben, haben wir jetzt keine geschaffen.

Larissa: Und der finanzielle Aufwand?

Alexandra: Der finanzielle Aufwand, also die im Gesetz angeführten Beträge, die ja auf die Betreiber wesentlicher Dienste äh zukommen werden, sind aus meiner Sicht bei weitem nicht realistisch. Äh in Deutschland gibt es beispielsweise Förderungen für die Betreiber von wesentlichen Diensten. Wäre auch in Österreich sehr zu begrüßen, da die Aufwände sicherlich erheblich sein werden. Wie erheblich sie sein werden, hängt davon ab was jetzt die zertifizierten Stellen was für einen Prüfkatalog sie haben. Ah ob sie sich an die Normen eben halten oder nicht. Und was unsere Vorschriften betrifft, da können die Aufwände schon sehr ins äh sehr nach oben gehen.

Larissa: Welche Verbesserungen sind aus Ihrer Sicht durch das NIS Gesetz zu erwarten?

Alexandra: Na ich erwarte mir eine rasche Information bei Bedrohungen, die die Informationssicherheit betreffen, ah eine unkomplizierte Kommunikation mit den jeweiligen Stellen, um gegebenenfalls auch rascher auf Informationssicherheitsvorfälle ah reagieren können.

Larissa: Wäre zu befürchten, dass die Zusammenarbeit ahm durch eventuelle Sanktionen geschwächt würde?

Alexandra: Das ist jetzt davon abhängig, wie die Behörde zukünftig damit umgehen wird. Man wird sehen (lacht).

Larissa: Welche Maßnahmen sind vorbereitend, also vor Inkrafttreten des NIS Gesetzes bei Ihnen in der Organisation getroffen worden oder mit der Wirtschaft etc.? Gibt es da was, das Sie benennen könnten?

Alexandra: Naja es ist… unsere Organisation wie gesagt stellt da die Vertraulichkeit, Integrität und Verfügbarkeit der uns anvertrauten Daten unserer PatientInnen auch ohne NIS Gesetz eine wesentliche Voraussetzung für unser Unternehmen dar. Ähm das sind Grundpfeiler für unseren Handlungsauftrag, für unseren Unternehmensauftrag. Auch die äh anvertrauten Daten unserer MitarbeiterInnen. Wir haben bereits vor dem NIS Gesetz dazu laufend Maßnahmen gesetzt und u.a. ein Projekt gestartet wie schon erwähnt. Innerhalb der Branche haben wir, in Vorbereitung des NIS Gesetzes und deren Auswirkungen, eine laufende Abstimmung gestartet.

Larissa: Befürworten Sie die Vorgangsweise der Europäischen Union, Sicherheit und insbesondere Cybersicherheit, gesetzlich zu regeln?

Alexandra: Also ich bin der Meinung, was die Meldepflicht betrifft, wird es ohne Gesetz wohl kein Lagebild geben. Von daher verstehe ich hier das staatliche Interesse. Hinsichtlich der Sicherheitsvorkehrungen, vor allem der verpflichtenden Nachweise durch wieder andere neue qualifizierte Stellen und zukünftigen Audits, finde ich, dass die Unternehmen doch sehr erheblich belastet werden können. Wie es dann schlussendlich sein wird, liegt daran, wie jetzt dann der Prüfkatalog ausschaut. Ahm das wird man sehen.

Larissa: Erfüllt das NIS Gesetz Ihre Erwartungen?

Alexandra: Also, ich erhoffe mir eine gute Kommunikation in beide Richtungen. Man wird dann sehen, wie sich das entwickelt. Ahm was die rechtzeitige Information im Falle von Cybersicherheitsvorfällen betrifft, kann das schon sehr positiv werden. Ahm weil wir bei einer guten Kommunikation auch schneller abwehren und Vorfälle beseitigen können. Also da kann es schon auch sehr vorteilhaft für die Unternehmungen werden.

Gut. Dann bedanke ich mich ganz herzlich für Ihre Zeit.

Alexandra: Bitte, gerne. Ihnen noch alles Gute für Ihre Bachelorarbeit.

Larissa: Danke.

9 Appendix 3 Interview Plessl

Interview Werner Plessl:

Larissa: For my bachelor thesis about the effects of the NIS law on Austrian companies, the operators of essential services, the following interview is conducted.

Do you agree on this interview being recorded and published? Are do you agree on personal data being published or do you want the interview to be anonymized?

Werner: Yes, I agree. May be published.

Larissa: Then I would like to ask you to briefly introduce yourself and to describe the organization and the field of activity which you are working in, please.

Werner: My name is Werner Plessl. At Hewlett Packard Enterprise, I am responsible for the, at least here in Austria, the Federal Ministry and the downstream departments, which have a sales responsibility, a corresponding team which supports me and assists me in serving the IT requests of the authorities and downstream departments. We are responsible for very important infrastructure systems together with the authorities, which must be supported accordingly.

Larissa: In your opinion, does the obligation to report contribute to get a better picture of the situation?

Werner: Yes. Definitely. I am one hundred percent convinced of that and would answer yes to that every time.

Larissa: In your opinion, can the cooperation between the state and the economy be strengthened, or are there negative influences of the NIS law noticeable for you?

Werner: Negative influences are not known to me at the moment. I can answer the first part of the question with yes.

Larissa: Will the reporting obligation also contribute to improve transparency?

Werner: Certainly, yes.

Larissa: Are you afraid that the reporting obligation will lead to negative headlines about your company?

Werner: Partly I would say yes, because if there are incidents and you have to report them, that is always connected with a risk. You can't say yes and no, so I would say yes and no, so in part this is certainly a negative assessment for the institution that carries out the reporting.

Larissa: Are you now only talking about obligatory reports or are you also afraid that, for example, the voluntary report will appear in the media?

Werner: Exactly. It is always about media presence in the end. In my opinion, voluntary reports happen rather reduced. Compulsory reports are only made when there is really, I would say, imminent danger. Yes, then there is the media effect everybody wants to avoid. That is really the insight I gain with customers when incidents happen.

Larissa. When you think back to the process of the creation of the law, how do you assess the cooperation between the state and the economy?

Werner: Right. So, in my opinion, the cooperation basically works well. I would have only wished that we were involved in all the relevant contents earlier. The earlier one is informed and can participate, the more efficient the outcome will be and one day both sides will benefit.

Larissa: So in your opinion, sector talks should have taken place earlier?

Werner: Exactly, they should have taken place earlier, maybe in a more intensive way, but in retrospect one is always wiser than before. But this is the first thing that can definitely be applied and can be used for the future.

Larissa: In your opinion, how has the implementation of the NIS law proceeded so far?

Werner: In the end that it happened rather quietly. It's not a wow-effect, which was supported by the media, but the law was activated and my presentation is that now you can observe and see how the whole thing starts and how it is used. This has been carried out very, very calmly and quietly.

Larissa: What arrangements have been made in your company to implement the NIS law?

Werner: Well, we are an international company and we have accordingly initialised a position called Chief Security Officer who also ensures that such laws and rights and obligations can be implemented directly and locally. Specific question; that is the answer. A CISO role has been created to deal with this kind of content.

Larissa: Does that mean that new jobs were created?

Werner: Well, not a dedicated worker as such, because that would not be one hundred percent capacity use somebody was dedicated to the NIS topic from Monday to Friday, from January to December, but a worker was created who has to serve several countries here. There is a network - Germany, Switzerland, Austria - of security officers who ensure that everything here is compliant. Such a role got created, but not a dedicated role in Austria.

Larissa: Were there any other changes within your company?

Werner: Changes are constantly happening here, namely with regard to process and sequence control in the case of cyber security incidents. So here we have created our own electronic education, where every HPE employee is obliged to take this course in order to create awareness of all the incidents that happen again and this training content must be repeated in a detailed framework. A source of information is repeatedly sent out by this CISO at certain points, which, on the one hand, indicates where one has to react to it and, on the other hand, also sends out fake information, where one can then see whether the employees are implementing it. One does not believe at all, how quickly people forget. The employees then see for example Do not press this button to give an example and then you just have to invite this employee again and repeat this training to emphasize the relevance again and to sharpen the awareness and this happens again and again. In other words, yes, training courses take place regularly to ensure that, if the need arises, there is controlled management and that we ourselves are always protected.

Larissa: What improvements can be expected from the NIS law from the perspective of your company or from your personal point of view?

Werner: Well, maybe I can catch up on what I said before. With regards to this NIS law we ourselves have also been sensitized and through these sensitizations and the associated improved procedures and processes that have also resulted in improvements for us. We really see the NIS law as a supplement to what we are doing in terms of the requirements that we have to meet as Hewlett Packard Enterprise. That was already a satisfactory act, this law. The question is just how much effort you have to invest in order to be able to really present a hundred percent complete solution. It's just an economic consideration of the interested parties.

Larissa: How do you assess financial expenditures caused by the NIS law?

Werner: Yes, exactly. This is something like judged? That is difficult. That is one. The expenses that arise here can't be quantified. We see it more as a proactive measure and try to prevent in case of damage, but it is difficult to evaluate it because it is difficult to put it into figures. You can only say that I am investing in the future in order avoid incidents and get the numbers to almost zero. The costs that arise from this are, let us say, manageable and profitable. But to bring that down to a figure, to say that it was now EUR 100 000 in 2018. That is the figure I cannot name.

Larissa: Not a specific number but was it significantly noticeable for your company?

Werner: Significant, no. Significant for me is always such a, such a peak, if you look at a stream of numbers, then you have a so-called anomaly, it was not something like that, nothing noticeable.

Larissa: Is there a fear that the cooperation with the economy would be weakened by sanctions, that is, that your company would completely refrain from voluntary reporting?

Werner: Sanctions are never good. Sanctions are never good and I am or we are a proponent of consensus. Yes, we love cooperation. We promote cooperation. Only together are we strong and I want to keep it that way.

Larissa: Do you support the EU's approach to legislate security, especially cybersecurity?

Werner: Of course, definitely yes. Together we will strengthen each other and I think it is only possible with a regulation like this. In principle, it is always to be questioned. I mean, you can also overregulate - no question. But with regard to this cybersecurity, that is absolutely to be advocated, yes.

Larissa: Does the NIS law meet your expectations?

Werner: (laughs). Of course.

Larissa: Then I would be at the end and thank you very much for your time.

Werner: Thank you very much for your time.

10 Appendix 4 Interview anonymous

Interview Anonym; Kritis:

Larissa: Für meine Bachelorarbeit zum Thema Auswirkungen des NIS Gesetzes auf österreichische Unternehmen, sprich in diesem Falle die Betreiber wesentlicher Dienste, wird das folgende Interview geführt. Sind Sie damit einverstanden, dass dieses Interview aufgezeichnet wird?

Anonym: Ja.

Larissa: Dürfen Angaben zu Ihrer Person veröffentlicht werden, oder möchten Sie, dass dieses Interview anonymisiert wird?

Anonym: Bitte anonymisieren.

Larissa: Gut. Dann komme ich zu den Fragen. Trägt die Meldepflicht Ihrer Meinung nach zum Gewinn eines besseren Lagebildes bei?

Anonym: (lacht) prinzipiell natürlich, ja, wobei die Meldepflicht an sich nicht einmal notwendig wäre, ja. Das NIS ist sicher ein wesentlicher Meilenstein für Unternehmen, Betreiber wesentlicher Dienst. Das zweite Thema, das auch sehr stark aus dem Bundeskanzleramt beziehungsweise aus dem BVT kommt, ist das Thema kritische oder strategische Infrastruktur, ja. Und über diese Ecken über diese Ecke hat die haben die Behörden einen relativ guten Überblick übern Markt, über Österreich, wo eigentlich eine kritische Infrastruktur vorhanden ist und wo kritische oder strategische Infrastruktur ineinander verzahnt sind, ja. Das NIS Gesetz würde jetzt in dem Sinne das Lagebild nicht verbessern, glaube ich einmal., ja, weils ja eigentlich schon das Thema strategische Unternehmen gibt, wo eigentlich die Behörden einen relativ guten Überblick haben über die Unternehmen und auch, wie die miteinander verzahnt sind, ja. Was natürlich wichtig ist, ist das ganze systemisch zu sehen, ja zwar nicht die Unternehmen isoliert, sondern die Abhängigkeit zwischen Unternehmen. Guter Bereich ist eh…also ein schönes Beispiel ist immer die Tankstelle als Beispiel, ja. Ohne Strom funktioniert die Tankstelle nicht, ja. Das heißt Energie, Kassa, Bankomat, ja. Ohne Strom funktioniert der Geldautomat nicht, ja. Vielleicht kurz, wenn überhaupt, wenn es irgendein Notstromaggregat gibt, aber im Großen und Ganzen

geht es immer um die Abhängigkeit zwischen einzelnen Industrien oder Industriesegmente, ja und wie sich das nachher auswirkt auf ein Lagebild, ja. NIS - das NIS Gesetz an sich ist sicher ein gutes Fundament, aber das Lagebild wird dadurch nicht verbessert. Nicht…nicht wesentlich verbessert. Sagen wir einmal so. Warum? Natürlich hat das NIS sehr stark die ITO Sicht und dadurch hat das natürlich auch eine Erweiterung zum typischen Unternehmensbegriff. Aber im Großen und Ganzen - Lagebild würde dadurch nicht wesentlich verbessert werden aus Sicht der Behörden.

Larissa: Würde die Meldepflicht dennoch dazu beitragen, Transparenz ein bisschen zu verbessern?

Anonym: Ja Transparenz nicht. Transparenz, ja. Mehr das Bewusstsein vielleicht auch von Unternehmern, ja die da reinfallen. Ich glaub dieses Transparenz, ja. Auch das Bewusstsein einzelner Unternehmen, dass sie hier eigentlich unter den Begriff Betreiber wesentlicher Dienste fallen, ja. Damit natürlich gewisse Maßnahmen treffen, damit sie dieser Begriff oder ja mit diesem Begriff diesem Bewusstsein einfach nachkommen, ja, dass sie hier Teil der ja Marktversorgung, ja als wesentlicher Betreiber sind sie im Prinzip wichtiger Marktversorger in Österreich, ja.

Larissa: Ja, also quasi ohne geht nicht.

Anonym: Genau. Im Prinzip, ja. Definitiv, ja.

Larissa: Befürchten Sie, dass es durch die Meldepflicht zu Negativschlagzeilen für Ihr Unternehmen kommt, wenn jetzt zum Beispiel eben drin steht…in den Medien berichtet werden würde, dass es in Ihrem Unternehmen ein Ausfall gibt?

Anonym: Nein. Nein. Nein, definitiv nicht. Definitiv nicht, weil wir haben sowieso als Markt- Markt- Markt- mir fällt das Wort nicht ein - als Marktteilnehmer Pflichten gegenüber den anderen Marktteilnehmern, ja oder Mitbewerbern, ja oder unseren Abnehmern Berichte abzugeben, wenn wir jetzt zum Beispiel Wartungen durchführen oder ähnliches, müssen wir sogenannte Remit Meldungen zum Beispiel abgeben ja. Also es ist zum Beispiel beim Strombereich ein Thema, genauso wie bei Gasversorgung, dass wenn es zu Wartungen kommt „ah Wartung - wird abgedreht“ muss es dementsprechende Remit Meldungen geben, ja - Meldungen an die anderen Marktteilnehmer, dass hier ein Versorgungsengpass einfach stattfinden wird in

Zukunft oder gerade stattfindet, ja in einem Notfall zum Beispiel, ja. Gut. Also das ist wirklich kein Thema. Also das ist für mich nicht mehr, nicht weniger, definitiv nicht, nein.

Larissa: Wenn Sie an den Entstehungsprozess des Gesetzes zurückdenken, wie beurteilen Sie die Zusammenarbeit zwischen Staat und Wirtschaft?

Anonym: Das kann ich persönlich nicht sagen, weil ich da eigentlich überhaupt nicht involviert war. Ich muss aber dazu sagen, dass ich damals noch in einer anderen Position war, dass eigentlich mein Chef sogar involviert war in diesen

Larissa: Sektorengesprächen?

Anonym: Ja genau. War natürlich das Unternehmen involviert, ja also ja, natürlich - man kennt sich ja im Sektor zwischen Unternehmen und Behörde. Man kennt sich ja und einfach aus dem Bereich strategische, kritische Infrastruktur schon heraus. Also man hat sich gekannt und man schätzt sich, ja. Es ist ein relativ gutes Miteinander, wo wir unseren Standpunkt auch einbringen haben können, ja und der auch so weit wie es Sinn macht, berücksichtigt worden ist, ja. Also im Prinzip ist es schon ein Miteinander gewesen die ganze Entwicklung in Österreich von dem Gesetz und dann der Vorordnung in weiterer Folge, ja.

Larissa: Wie ist die Umsetzung des NIS Gesetzes aus Ihrer Sicht bisher verlaufen? War es einfach für Ihr Unternehmen, die Maßnahmen zu integrieren oder war es doch ein größeres Struggle?

Anonym: Nein, nein, nein. Der Punkt ist vom Prozess her ist die Verordnung letztes Jahr, vorletztes Jahr, na letztes Jahr erst in Kraft getreten und das Thema ist jetzt, was wir bekommen haben oder noch nicht bekommen haben, ist natürlich, das kommt jetzt auf den Bereich drauf an, auf den Bescheid. Ich meine, wir wissen natürlich, welche Anlagen hier im Prinzip unters Gesetz fallen, ja, aber es gibt bis jetzt noch keinen Bescheid. Später wenn dann der Bescheid da ist, hat dann das Unternehmen per Gesetz drei Jahre Zeit, sich einen…eine qualifizierte Stelle auszusuchen, der uns nachher als Unternehmen dann in diesem Falle prüft, der den NIS Audit durchführt. Das heißt, so richtig ist noch nicht das NIS Gesetz gelandet, es fehlt noch der Bescheid. Wir müssen natürlich den ganzen Prozess durchgehen. Der Gesetzgeber schlägt ja vor

oder, man spricht da von einer regelmäßigen Zertifizierung, ja, dass wir als Betreiber wesentlicher Dienste alle drei Jahre im Prinzip uns auditieren lassen, damit wir auch wirklich diese ISO2700irgendwas oder das ISO

Larissa: BSI Grundschutz und so weiter, ja, ja. (lacht)

Anonym: Ja, ja, genau. Im Prinzip sind wir noch am Weg dorthin, also diese Reise ist im Prinzip noch nicht abgeschlossen, ja. Bis jetzt ist es okay. Es ist, wie es ist, ja. Äh, ja.

Larissa: Okay, dann eine Frage noch: Wie wie woher wissen Sie, ob oder dass Sie Betreiber eines wesentlichen Dienstes sind, wenn Sie noch keinen Bescheid erhalten haben?

Anonym: Also erstens einmal hatten wir die Sektorengespräche…

Larissa: Ja, gut. Stimmt.

Anonym: …wo sich dann herauskristallisiert hat in erster Linie. In zweiter Linie haben wir Kontakt ja auch zur Behörde, beziehungsweise in der Verordnung steht auch drin welche Betreiber, welche Kriterien da auch drunter fallen und welche nicht. Also das steht in der Verordnung drin und das kann man sich schon ausmachen. Also wie gesagt, wurde ja schon im Vorfeld mit der Behörde drüber geredet, ja. Es ist keine Überraschung, ja, dass wir demnächst den Bescheid bekommen, beziehungsweise für Bereiche schon einen Bescheid bekommen haben, ja.

Larissa: Ja, gut. Mich überrascht es auch nicht dass Sie Betreiber eines wesentlichen Dienstes sind, ehrlich gesagt. Das hätte ich auch so schon vermutet gehabt.

(beide lachen)

Anonym. Nein, nein, muss man muss man differenzieren im Prinzip, wer hier..ja

Larissa: Aber man kann sich's an den Schwellwerten und so weiter: Man kann es sich schon erschließen.

Anonym: Genau. Richtig. Genau so ist es. An den Schwellwerten merkt man es schon. Das stimmt.

Larissa: Welche Vorkehrungen wurden in Ihrem Unternehmen zur Umsetzung des NIS Gesetzes getroffen? Gab's vorbereitend irgendwelche Maßnahmen oder sobald Sie gewusst haben, Sie müssen sich ans Gesetz halten? Gab es da Maßnahmen, die integriert werden musste, um sich ans NIS zu halten.

Anonym: (seufzt)

Larissa: Oder kam es innerhalb der Organisation zu Veränderungen?

Anonym: Nein. Naja, es ist natürlich schon der Fall, dass man durch die NIS Verordnung natürlich in gewisse Bereiche mehr reinschauen, ja. Wir schauen uns dort natürlich schon den NIS Katalog oder Maßnahmenverordnung an auf gewisse Punkte, worauf man halt schauen muss. Das fängt an beim elektronischen Zugriff auf Systeme, ja und die Systeme müssen dementsprechend auch restriktiv auch gehandhabt werden…Anlagen, physischer Zugang, Zugriff und Zugang auch auf die Anlagen, ja. Es muss ein Managementsystem für Notfallkrisenmanagement etabliert sein und dergleichen, ja. Der Punkt ist, jetzt haben wir Gott sei Dank alles, ja. Man muss das definitiv noch ein bisschen im Detail anschauen, ja. Und was wir schon machen nachher, da wo es schon Teile gemacht ist, wir sind ISO zertifiziert, ISO 27, ja und damit haben wir eigentlich nichts zu tun. In dem Bereich, wo wir eben nicht ISO-zertifiziert sind, 2701, dort muss man nochmal reinschauen, ob man nicht noch Managementprozess zum Thema Riskmanagement, Securitymanagement, IT oder ITO, (nicht verstanden) Prozess aufsetzen muss. Um diese Risikoanalysen durchzuführen, passieren natürlich nach den entsprechenden Standards, die Maßnahmen entsprechend umsetzen und so weiter, ja. Prinzipiell, das Fundament ist da. Man muss halt dementsprechend an der einen oder anderen Stelle noch nachschrauben oder nachjustieren, ja.

Larissa: Sind dafür eventuell neue Arbeitsplätze geschaffen worden? Oder..

Anonym: Na, na. Nein, eigentlich nicht, nein.

Larissa: Okay.

Anonym: Wobei jein. Was natürlich schon stark der Fokus war auf IT, ja, Informationstechnologie, was natürlich schon mehr in den Fokus und wo eben auch

ein Zusammenrücken ist zwischen IP und OP, ja. Das ist schon, die ganze Operations Technologie, ja, die Anlage vor Ort mit der ich mit Pumpenventil und dergleichen, ja. Da gib es natürlich auch Systeme, computerbasierte Systeme, ja , dass diese Gassysteme computerbasierte Systeme, die jetzt natürlich auch mehr in den Fokus rücken, ja. Dadurch gibt es sehr wohl. Ich mein, das ist jetzt nicht unbedingt NIS bezogen. Das ist generell natürlich Thema Cybersecurity, ja, wo es natürlich schon stark in äh in Security Oficce, Cybersecurity Office, ja. Dann gibt es OT Security Officer. Es gibt immer mehr diese fancy Rollen, ja, die's jetzt schon gibt, aber jetzt nicht unbedingt wegen dem NIS Gesetz, sondern generell, weil der Markt hier einfach schon in die Richtung geht, ja. Cybersecurity ist ein wichtiges Thema, über die letzten Jahre immer präsenter und präsenter geworden, ja. Für die Risiken ist es unter den Top 5, ja. Also das ist schon hm, ja. Und dadurch sind natürlich sind Positionen oder Arbeitsplätze äh erschaffen oder geschaffen worden, aber nicht unbedingt wegen dem NIS. Man könnte schon aus der NIS Gesetzgebung eventuell heraus neue Arbeitsplätze eventuell auch, wahrscheinlich eher mehr aus der Ecken qualifizierte Stelle. Da gibt es dann nachher die Berater wie TÜV zum Beispiel, ja, die natürlich als qualifizierte Stelle, ja, im Prinzip die Unternehmen, wesentliche Dienste auditieren können, ja. Aus dieser Ecke heraus ja, gibt es natürlich zusätzliche Geschäftsmodelle und aus dieser Ecke wurden sicher zusätzliche Arbeitsplätze geschaffen. Also unterm Strich definitiv mehr Arbeitsplätze, ja.

Larissa: Ist für Sie zusätzlicher finanzieller Aufwand entstanden?

Anonym: Ja. Definitiv, ja, weil wir natürlich die Risikoanalysen bei uns für Bereiche für externe Partner machen, um uns auf diesen Audit vorzubereiten, ja. Damit ist definitiv ein Mehraufwand auch ja geht Hand in Hand, ja.

Larissa: Können Sie den beurteilen den finanziellen Aufwand? Bemessen? Mit hoch, niedrig, schwerwiegend…? Ist uns eigentlich egal?

Anonym: (lacht). Na, egal ist es nicht. Es ist auch nicht schwerwiegend. Es ist eigentlich teilweise schon vom täglichen Geschäft fokussierter, sagen wir einmal so, ja. Da ist natürlich mehr die Kommunikation die Thematik, ja, Abwicklung von Risikoanalysen und dergleichen. Da ist es…man hat ja einen externen Berater, der uns unterstützt ja in einer Phase zwei, drei Monate. Also der Aufwand des Beraters natürlich und dann

intern natürlich die Stunden, die noch auftreten, um eben diese Analysen durchzuführen, ja, ISO27 compliant ja in gewissen Bereichen oder nicht, ja. Der Aufwand ist für Unternehmen, ja, es ist bezifferbar, aber er ist nicht groß, eher klein. Aber es ist ein zusätzlicher Aufwand, er ist jetzt nicht weiß ich wie riesig, ja. Man könnte sagen das sind zwei Monate Beraterstunden, ja, plus nochmal intern das Gleiche nochmal an zusätzlichen Stunden, wenn man so sagen will, ja. Kann man so sagen, pi mal Daumen, aus der Hüfte geschossen, ja.

Larissa: Mhm. Wär zu befürchten, dass die Zusammenarbeit mit der Wirtschafft durch Sanktionen, die eventuell auf Sie zukommen könnten, geschwächt würde?

Anonym: Ah, durch das NIS.

Larissa: Genau.

Anonym: Na, ich war jetzt grade woanders. Nein, definitiv nicht. Wir sind gut aufgestellt, unsere Anlagen sind in dem Sinn State of the Art, nein. Da sind überhaupt keine Sanktionen. Natürlich, das stimmt schon, diese Befürchtungen hat es gegeben, ja. Diese Befürchtungen hat es vorm NIS Gesetz schon gegeben im Bezug auf äh auf Diskussion was ist eine strategisches oder kritisches Unternehmen, ja. Da hat es schon die Diskussion gegeben, welche Anlagen fallen unter den Begriff strategisches Unternehmen oder kritische Anlage, ja. Da hat es sicher die Diskussion gegeben, also da wird zusätzlicher Mehraufwand kommen, aber das muss man sagen, hat sich im Prinzip bis jetzt noch nicht befürwortet also nicht ergeben. Tatsächlich, generell natürlich durch die zusätzliche Bedrohung Cybersecurity, ja, ist natürlich ein Mehraufwand gegen für Unternehmen, ja, aber das ist unabhängig von der NIS Gesetzgebung.

Larissa: Welche Verbesserungen wären durch das NIS Gesetz aus Sicht Ihres Unternehmens zu erwarten? Oder sind schon eingetreten vielleicht?

Anonym: Ja, Prozesse werden optimiert, Prozesse werden harmonisiert, es wird natürlich das Unternehmen wird besser verstanden, ja, also das Thema, ja. Das geht eigentlich mehr in Richtung Business-Continuity eigentlich, wo man sagt „Was sind unsere kritischen Prozesse, ja, welche Anlagen was, wie schauen die Prozesse aus, was brauch ich da für einen Input, Output, was sind meine Ressourcen, die diese Prozesse

im Prinzip auch am Leben erhalten.“ Also, dass man auch wieder ein bisschen mehr dieses Bewusstsein zu bilden, ja, also was sind unsere kritischen Prozesse, kritische Anlagen, ja, wie schützen wir diese Anlagen, ja, aus die Ecken heraus äh ja. So, jetzt hab ich die Frage nicht verstanden. Jetzt hab ich die Frage vergessen hahahaha.

Larissa: Welche Verbesserungen Sie erwarten? Es klang danach, als befürchten Sie in Ihrem Unternehmen eigentlich keine Ausfälle.

Anonym: Na, na, na.

Larissa: Beziehungsweise auch nicht einmal, dass Sie irgendwie überhaupt Meldungen absetzen müssten.

Anonym: Meldungen absetzen Richtung Behörde, naja der Punkt ist schon, muss man schon also was niemand, vor allem haben wir jetzt gerade gesehen mit der Cyberattacke aufs Außenministerium, ja. Es ist niemand gefeit, dass er attackiert, dass es eine Cyberattacke gibt. Aber auch private also Unternehmen haben können immer irgendwie Ziel einer Cyberattacke sind, ja, sein. Und dass man da natürlich eine Meldung abgeben muss oder soll, ist natürlich klar, ja. Aber im Großen und Ganzen sind wir aber gut aufgestellt, ja. Aber Fremd… Fremdeinwirkung können wir nie ausschließen. Sagen wir es einmal so, ja. Aber intern sind wir eigentlich sehr gut aufgestellt, wo man eigentlich keine Ausfälle äh erwarten oder erhoffen, sagen wir einmal so, ja.

Larissa: Befürworten Sie die Vorgangsweise der EU, Sicherheit, insbesondere Cybersicherheit, gesetzlich zu regeln?

Anonym: Hmmm nein. Insofern nicht ich hab’s gesehen, wie’s unsere Behörde gemacht hat, die österreichische Behörde im Bezug auf kritische strategische äh Infrastruktur. Da war das wirklich auf gleicher Augenhöhe eine Kommunikation, ein Informationsaustausch, da braucht es braucht keine Gesetzgebung, ja. Das ist der Punkt dahinter. Es braucht es schadet vielleicht nicht, ja, aber es nicht notwendig. Die Frage ist, ob das nicht zu viel Aufwand eigentlich ist, ja. Wir reden jetzt da nur für IT Systeme, ja. Das ist das nächste, ja. Na, ich glaub eher nicht, na. Ich befürworte das nicht. Es geht auch ohne Gesetz genauso.

Larissa: Erfüllt das NIS Gesetz trotzdem Ihre Erwartungen?

Anonym: (seufzt) Ja, der Vorteil ist natürlich schon, es ist sehr transparent, Das muss man schon sagen aus der Ecken heraus, ja ist es schon nachvollziehbar und ja als Gesetz ist es definitiv, was ich mir erwarte von einem Gesetz, ja. Es ist relativ klar. Es ist klar im Prinzip, welche Unternehmen drunter fallen, welche nicht. Also das ist da ist nicht recht viel Raum bezüglich Interpretation, also das erfüllt so als Gesetz definitiv den Sinn und Zweck, ja. Definitiv, ja.

Larissa: Gut, dann bin ich am Ende meiner Fragen und bedanke mich sehr herzlich für Ihre Zeit.

Anonym: Danke sehr. Ebenfalls, danke.

11 Appendix 5 Interview Gwehenberger

Larissa: As part of my bachelor thesis, I am now conducting this interview. Do you agree that this interview will be recorded and published?

Erik: Yes.

Larissa: Accordingly, I would ask you to briefly introduce yourself, as well as to describe the organization you work for and explain your role in it.

Erik: My name is Magister Erik Gwehenberger. I am working in the BVT, i.e. BMI -BVT, more precisely in the department NIS and I work on the implementation of the NIS law and comparable legal matter.

Larissa: Then I would start with the first question. How has the implementation of the NIS Law been so far from the perspective of the authorities?

Erik: The implementation has been very positive so far. There is good communication with the affected companies of the respective sectors. There is also a very good cooperation with the Federal Chancellery from our point of view. We are still within the initial stage, but all in all one can report of a positive course.

Larissa: Does the NIS law meet your expectations?

Erik: The NIS law is based on the so-called directive of the European Union, simply said, its present configuration is a compromise solution. I was also part of the legislative working group of the NIS Law.

Larissa: What was your task area?

Erik: I was a representative of the BMI, yet I was not an official representative of the BMI, but I provided technical input on how to implement the NIS-Directive in the best possible way within the country. As I said, the NIS-Directive is a compromise solution, it was a first step, but there is a logical need for improvement. But so far, the NIS law

is a very important first step to strengthen cybersecurity in Austria and also in the EU through the NIS-Directive.

Larissa: Do you see any deviations from your expectations?

Erik: m The NIS-Directive currently only covers seven sectors and it has been decided in Austria that you take over these seven sectors in the form. I am moving forward to the next question; goldplating has never been an issue. In my opinion, one could have included other areas here, but that would be a political decision that has been made.

Larissa: So, no goldplating has been done?!

Erik: No goldplating in the traditional sense. The only thing involved was the public sector. There are so-called federal institutions, public administration institutions, to set a good example, because there is no point in obliging the private sector to fulfil all measures set by the NIS but leaving the public sector out.

Larissa: Has the transposition into national law taken place as planned or was the target overshot?

Erik: In terms of timing, no. It could not be implemented in a timely manner because the NIS-Directive provided that by 9th May 2018, it should have been transposed into national law. Austria did not do that until the end of 2018. This delay in time was the only thing.

Larissa: What improvements can be expected from the NIS law?

Erik: First of all, that the affected companies now have the legal obligation to deal with cybersecurity. Hopefully that will also cause a cascade effect. This means that a state will hopefully emerge, i.e. the companies affected will be dedicated to the subject, but also, for example, small and medi-sized enterprises, which are not covered by the NIS law, ... it simply adds value to deal with cybersecurity from a business´ standpoint. Considering the exorbitant amounts of damage that can be caused by cyber-attacks or security incidents, it is obvious that the issue is becoming more important, both domestically and internationally.

Larissa: When you think back to the law-making process, which you were involved in, how do you assess the cooperation between the state and the economy?

Erik: I don't want to praise ourselves, but this was an excellent example of how you can involve the economy in the process of creating a law. That is not the usual case in terms of how that happened and it would be desirable if that was done in other areas as well.

Larissa: Could you explain that a little bit more?

Erik: Yes. , there were several rounds of so-called sectoral talks in the course of the legislative process where at that time potentially affected companies were invited, sector representatives, sector associations, departments, other departments that are responsible for possible companies, for example the BMVIT, the Ministry of Transport for the ÖMV, ASFINAG and so on. They really tried to work out a balanced solution together or to get input from the respective sectors in order to work out a balanced solution in order to get a correspondingly presentable result in the end.

Larissa: How is the cooperation with the economy, in this case with the operators of essential services, from the authorities' point of view, so from your point of view?

Erik: From the present point of view?

Larissa: Yes.

Erik: We have to say that most of the sectors are currently under investigation. Only the sector drinking water is ascertained. This means that this area of investigation is of the Chancellor's responsibility.

Larissa: A short interposed question: The sector of drinking water supply is ascertained. Does this mean that the operators of essential services in the drinking water sector are already elected? Do I understand that correctly?

Erik: Exactly. They have been determined by the Federal Chancellery through official channels in the meantime by an official decision. This means that they received the status of operators of essential services according to the NIS law.

Larissa: That implies that the companies have de facto received the notification and are aware of the fact that they are operators of essential services?

Erik: Yes.

Larissa: Okay. What measures have been taken preparatory, involving the economy?

Erik: Yes, just these same sector talks. There were also some bilateral talks, respectively trilateral talks between the BMI, Federal Chancellery and possibly affected companies, or with the Chamber of Commerce and so on and so on. So in short, the business community and the private sector has been sufficiently informed. In addition, I must also say that we, and I am now speaking on behalf of our presentation, have held countless lectures on this topic over the past one and a half or two years and have really tried to give the topic a stage in the minds of the companies concerned or the topic itself.

Larissa: Why are qualified bodies established and what are the criteria for accreditation?

Erik: They have decided on this system, since there already is an existing market of companies which are dealing with this subject testing, so there is no need to invent a new system when there is an established system in place. The only innovation is that we determine the suitability of these qualified entities, i.e. of these respective companies, and the requirements result from the Ordinance on Qualified Bodies, in short the Tassel Ordinance, where these requirements are laid down, and we examine on the basis of these requirements whether the respective company which submits an application to us is suitable to act as a qualified entity in the market.

Larissa: What criteria were used to select the minim safety standards?

Erik: Well, there were a lot of considerations on the European level, but this led to the fact that there is a so-called NIS Cooperation Group, a body in which the member states are represented, which deals with the topic of NIS and cyber security. They also developed a paper in cooperation with the ENISA, where established standards, which are currently in use, such as ISO 27001, BSI IT basic protection and so on and so on, more or less in a mapping table evaluated and in addition to there was also a docent,

where individual security measures, that is to say, the term used in the NIS system, were described and were then taken from this and austrophied. That means more or less adopted, but the one or the other point was specifically adapted.

Larissa: According to which criteria were the threshold values defined?

Erik: There are several types of thresholds. There are the thresholds for identifying whether one is an operator of essential services at all, and then there are thresholds that determine when an incident has reached a certain quality, is therefore a so-called security incident, and therefore a mandatory report must be made. This has been tried to be established in the context of these sectoral talks and the regular exchange of information with the industry, and was then incorporated into the NIS regulation, that is, the regulation in which the threshold values are found by the Federal Chancellery.

Larissa: Are frequent sanctions to be feared?

Erik: Hopefully not. Because it is an administrative matter and because the NIS directive also allows for it, there are sanctions at the end of the NIS law. We hope that there will be no need to use these penalties, because we believe in good cooperation between business and authorities and it will not come to that.

Larissa: Otherwise, would there be any fear that the cooperation with the economy would be weakened by such sanctions?

Erik: The danger exists at least theoretically, but the companies are aware - this is common practice in administrative matters, for example - that the state imposes certain obligations and imposes sanctions if these obligations are not implemented. This is not a new system that is being established, and the penalties are also set within a framework that is understandable and there is a lot that would need to happen to actually have a penalty payment, because there are certain mechanisms in the law in order to give the companies concerned the opportunity to compensate for abuses before a penalty is even imposed.

Larissa: In your opinion, does the obligation to report contribute to get a better picture of the situation?

Erik: Yes, absolutely, but it has to be said that the obligation to report refers to cases that are really from a qualitative point of view really ...

Larissa: Serious.

Erik: Serious. From our point of view, we hope that the so-called right to volunteer... Well, we like to call it the right to voluntary reporting, because, as far as the NIS law is concerned, from the point of view of data protection law you have the possibility to report incidents or risks which will eventually lead to...or hopefully lead to a better overview, to a better picture of the situation in the individual sectors and also throughout Austria and, we must not forget, throughout Europe. That is the idea of really establishing a Union-wide system, where we can actually react quickly if security incidents occur.

Larissa: Are any negative influences of the NIS law noticeable or can the cooperation between state and economy be strengthened?

Erik: At the moment there are no negative effects noticeable yet. We hope that the cooperation will simply be maintained. We also really try to approach the affected companies in a cooperative way. Therefore, from the current perspective, no. Well, there are no noticeable negative influences.

Larissa: In your opinion, will the reporting obligation help to improve transparency?

Erik: At the beginning, where this reporting obligation was discussed, the companies' argument was always "Yes, but what happens if this is taken up by the media? , if it is then so to say exploited in the media. The reputation of the respective company could suffer and so on and so forth."

Larissa: Short interposed question; for example fictitious theoretical example: ÖBB is identified as an operator of an essential service in the field of transport and all trains are cancelled and in the media it says exactly that and therefore the reputation of ÖBB suffers.

Erik: Yes. This is hopefully a fictitious case, where a mandatory notification has to be made, also according to the criteria that are now being defined, now regardless of whether ÖBB actually is the operator of essential services and so on. But yes, and

there the argument has come up, that if this reporting channel or the reporting system is not regulated properly, then the reputation of the company could possibly be damaged, if before the responsible Ministry of the Interior possibly before the Ministry of the Interior receives the report that you are already reading in the newspaper, possibly with false information and so on and so on. However, there has been a paradigm shift in the meantime in that companies have realised that it is not the end of the world when an incident occurs. It rather depends on how you react to it. It's more like...well the paradigm shift has moved from profiling to reacting and companies are more likely to be judged by how they react to an incident; how they interact with their customers... how they inform their customers...how they react to it and how they communicate. So far, there is no company is a Fort Nox that you can't attack.

Larissa: Finally: What further steps do you think should be taken by the EU?

Erik: Yes, at the moment, it can be seen that there is a danger that there will be a, how shall I put it, a fragmentation in the field of cyber security. This means that the issue of cyber security is being regulated in parallel in several areas. This naturally entails the risk that companies could be subject to multiple obligations, but I hope that the EU, and in particular the Commission, will be aware of this and that progress will be made towards adequate harmonisation in this area. It is also the case that the NIS Directive will be evaluated after five years.

Larissa: By whom?

Erik: By the Commission. By the European Commission. And since it can be assed that the NIS Directive in its current form will be adapted.

Larissa: Adapted in what respect?

Erik: Yes, the Commission is now trying to evaluate within these five years how the measures have been implemented in the different member states and since one can say that there are differences in the implementation and that the Commission will them into account and possibly adapt the NIS Directive in such a way that it will not give the member states as much leeway in the transposition into national law. That is quite conceivable.

Larissa: In the way that the comparability from one EU country to another will also be enhanced.

Erik: Becomes better, exactly.

Larissa: Well, thank you very much for the interview and your time.

Erik: My pleasure.

12 Appendix 6 Interview Maier-DeKruijff

Interview questions MMag.Heidrun Maier-DeKruijff:

In your opinion, does the reporting obligation contribute to get a better picture of the situation?

Yes, the reporting obligation contribute to get a better picture. Companies receive information about new attacks and especially about unknown types of attacks in a timely matter and can therefore protect themselves in a better way. Furthermore, concealing incidents in companies is for more difficult than before.

Can the cooperation between the state and the economy be enhanced by the obligation to report or are negative influences of the NIS Act noticeable?

The reporting obligation can improve cooperation between the state and the economy. I didn't observe that the cooperation between our member companies with the state is negatively affected by the NIS Act. Good cooperation is particularly necessary on an important issue such as security of network and information systems and I am sure that companies see it that way. Both the regular exchange with the state and certain obligations formulated in the Nis Act have already been implemented before the NIS Act was enacted.

Will the reporting obligation contribute to improving transparency?

There is no improved transparency for us as an association. It is certainly different for companies, because they are informed and warned about incidents.

Are you afraid of the reporting obligation leading to negative headlines for your company?

No, because my association is not subject to the NIS Act and therefore, we are not subject to the reporting obligation. However, it can of course lead to negative headlines for companies who are subject to the NIS Act, if they don't deal with the topic of cyber security and ignore the requirements of the NIS Act. In the end, the

reporting obligation may as well be an opportunity to learn from mistakes or carelessness of others.

When you think back to the law-making process, how would you assess the cooperation between the state and the economy?

It was a normal legislative process in which we, as well as some of our member companies, used the opportunity to submit comments on the draft.

In your opinion, how has the implementation of the NIS Act proceeded so far?

In my opinion, the implementation by our member companies has gone very well so far. Many of our member companies are very well positioned in the cyber security sector and have therefore already fulfilled many of the requirements before the NIS Act was enacted. Furthermore, some of the companies have already been subject to similar regulations in other directives.

How do you assess the cooperation with the authorities so far?

My association cooperates very well with the responsible authorities and has also been able to organise workshops with employees of the responsible authorities for member companies subject to the NIS Act.

What precautions were taken in your company to implement the NIS Act?

As we are a non-profit association and we are not an "operator of essential services", we are not subject to the NIS Act. Therefore, we have not taken any precautions.

Have there been any changes in the organisation of your company?

No, because we are not subject to the NIS Act. I am not aware that there have been any changes in member companies

Were new jobs created for this purpose?

No, not in my association. In our affected member companies the IT or ICT departments and employees have taken charge of this topic.

What improvements can be expected from the NIS law from your company's point of view?

Welche Verbesserungen sind aus der Sicht Ihres Unternehmens vom NIS-Gesetz zu erwarten?

My association is not affected, therefore I can't make an assessment.

How do you assess the financial expenditure caused by the NIS Act?

I have no insight into the financial expenditure of our member companies, so I can't answer this question.

Is it to be feared that the cooperation with the economy will be weakened by sanctions?

No, I don't think so, because companies want to keep sanctions low and good cooperation is the best way to influence them.

The sanctions in the NIS Act are necessary as a means of exerting pressure on companies to implement the committed security requirements.

What preparatory measures were taken with the involvement of industry?

Do you support the EU's approach to regulate security, especially cyber security, by law?

Yes, because there are probably many organizations that would not take cyber security seriously without laws. Especially small companies tend to assume that they are not in danger of an attack, because of their size, which is not true.

Another point is that only through harmonized regulation in the EU, can we generate a uniform level of security.

Does the NIS law meet your expectations?

Yes, in my opinion points such as the reporting obligation are positive because companies can benefit from it and a chain reaction of attacks can be avoided. A uniform level of security in Austria and throughout the EU is also very good.