Deliverable: Analysis of Individual Criteria

IT Infrastructure Maturity

by

Dale P. Bada

Submitted for Assessment in

UC1ST1103 - Studio 1

at

Noroff University Collegge

Noroff
School of technology
and digital media

Contents

1 Introduction

Subject: UC1ST1103 - Studio 1

1.1 Document Information

Studio1 project deliverable:	Analysis of individual criteria
Topic/Subject of analysis:	Critical Infrastructure Maturity
Word count:	N/A
Estimated read time:	HH:MM
Pages:	14

1.2 Course Lecturers

Course leader:	Prof. Mariya Chirchenkova Prof
Course lecturer:	Prof. Rayne Reid

1.3 Subject Matter

This paper is an analysis of Norways Cyber Security posture. We will delve into; "How Cyber Security addressed in the area of Critical Information Infrastructure from policy and legislative standpoint". How Cyber Security affects a nations, any nation, and its citizens? We will examine the challenges of most imminent import. And assess what lies further in the foreseable future. We will address the above topics From the perpective Norways national Cyber Securities interest.

The latter part of the paper is a comparrable analysis of Norways National Cyber Security Strategy with its peers within the European Union. The basis of comparrison will focus on a selection of strategic imperatives as outlined by ENISA [1], in their "NCSS"[2] Good Practice Guideline.

One focus area is on the analysis involving "Critical Information Infrastruture"; the underlying systems which provides services that everyone relies on, on a daily basis. Heed the previous statement as indication to how broad and vast the topic is. Therefore the necessetity to constraint on 2 specific area or industries.

Cyber Security concerning:

- The financial industry
- The telecommunication industry

The countries subject to analysis and comparison are:

- Norway

[1] European Union Agency for Cybersecurity
[2] National Cyber Security Strategy

- Sweden
- Denmark
- Finland
- Iceland
- United Kingdom
- Russia
- France
- The Netherlands
- Bulgaria

The countries are selected on the basis of:

- Geographical vicinity
- Similarities and/or contrastring traits in:
  - IT infrastructure maturity
  - IT services utilization
  - Culture
  - Geopolitical profile
  - (Assumed) Cyber Security posture
  - Compliance level (according to ENISA's NCSS Good Practice)

1.4 Exclusions

The exact definition of what entails "Critical Information Infrastruture" is a fundamental necessetity to have established. It is therefore throughly outlined in the guidelines and directves used as source materials this analysis is based on.

This paper follows the source materials' definitons of "cyber security", financial industry and telecommunication industry. Other industries and security concerns may be mentioned, but not be the focus of the analysis.

Other countries, than the 10 listed above, maybe mentioned or referenced, but are otherwise not the focus of the analysis and comparison.

Details regarding the policies and legistations relevant to Critical Information Infrastructure and the Financial sector will be referenced. The full detail will not be outlined in this document.

1.5 Circle of trust

There is no 1 solution that can be implemented and enfoced to attain a 100% secure any physical or digital entity. Information Security requires many layers of cleverly designed technical solutions and implementations. Be it a preventive or a more offensive counter measure.

However, an important, but often neglected part of Information security are the non physical and non technical layers and aspects of information security. These are the overarching best-practices, standards and legislations that impacts, and many cases sets precedence over, the technical solutions.

There will always be a trade-off in terms of accepted risk, exposure, convenience and accessibility. And limitations to address in terms of human skill, time, IT resources and funding. Just to name a few.

In this paper, we will examine how a Norway and other European Unions states approaches the issue of information secruirty from policy and legislative point of view. It will also discuss how to improve current standings of current policy and delve into some technical solutions that may help reach the policy objectives.

2 What accounts for a successful Cyber Security Strategy?

There are many components, layers and moving parts that needs to be addressed for a successul implementations of a National Information and Cyber Security Strategy.

- International standards and policies
- Regional standards and policies
- Natioanl standards and policies
- Sector (private or public) policies
- Industry standards, best practices and policies
- Technical education, proficiencies and comprehentions
- Technical solutions and systems implementations
- Utilization solutions and enforment of policies

Information and Cyber Security is, as with any complex and interconnected systems, only as strong as its weakest link. Requiring all of the components, or layers, listed above to be designed, implemented and function seemlessly together in order to have a solid baseline[1] for a National Information and Cyber Security Strategy.

At the very top, and in many cases the starting point of all consequtive items in the list, are the standards and policies defined by the European Union and its individual Member States. A piece of paper, a signed law that starts it all, and mandates action to be taken.

To understand current objectives and standings of Norways Cyber Security Strategy, and its couterparts in the European Union, we need to understand the history behind the strategies itself. The challenges and events that promted for such a strategy. The stakeholders involved, and the policies and regulation derived from the inital effort.

After tracing back the initiative's history and understanding its requirements and objectives. We will be able to understand strategy's current form, the policies derived from it. And the agencies and organizations that was established to implement, monitor and enfoce the strategies. Basically the; who, when, why and how.

2.1 The European Union's NIS Directive and its Annex

On the 6th of July 2016, the European Union [2] has approved and signed off on The Directive on security of network and information systems (NIS). It is a legislation affecting all European Union member states, and its trading partners in the European Single Market [2]. All EU member states are mandated to "tranpose", or incorporate the directive into their National legislations by 9th of May 2018. In the 2nd of October 2020, a review of the Directive has been conducted, and a revised NIS has been presented to the European Comission on 6th of December 2020.

The Directive has 3 annex documents. The annexies provides more context and clarity to the Directive.

- Annex 1

[1] With the emphasis on "baseline", as a 100% security cannot be achived without implications to other aspects such as usability, interoperability and efficiency. There are trade-offs and comprimises at all levels.

[2] more specifically: the European Comission proposes a Directive, a bill of law, and the EU Council and thhe EU Parliament deliberates and votes if the new Directive or bill will pass, be approved.

[2] https://en.wikipedia.org/wiki/European_Single_Marketformoredetails

  - Provides guidance to the tasks and clarification of the requirements pertaining to the NIS Directive.

- Annex 2

  - Identifies the sectors and subsectors considered as higly critical in provisioning the services for each Member State and the Union as a whole.

- Annex 3

  - Outlines the services regarded to essential for the functioning the population for each Member State and the Union as a whole.

Where the Directive can be regarded a as formal legislative document, with the language to match. The annex documents explains and expands on the task, requirements and scope of the Directive with a language that matches its intended audience.

2.1.1 NIS' objectives

According the the NIS Corrigendum, European Commission, 2017 , a communication by the European Commission to its Member States, the Directive has 3 main objectives:

- Improving nationanl cyber security capabilities,

- Building cooperation at EU level, and

- Promoting a culture of risk management and incident reporting among key economic actors, notably Operators of Essential Services (OES) for the maintenance of economic and scietal activities and Digital Service Providers (DSP).

However, each Member State are expected to expand on the 3 main objectives, and define its NCSS according to each Member State's specific needs and priorities as long as it is never below the requirements and objectives set in the NIS Directive.

2.1.2 NIS' scope

As indicated in the list above, Annex 2 and 3 outlines the scope of the directive. The Directive does not describe in detail what the scope is. Instead the Annex provides a guideline to identify what constitutes a Operators of Essential Services (OES), as can be read in Section 4.1 in the Annex 3 OES. As of 16th of December 2020, NIS2[4] proposal has been sent to the European Comission expanding the scope of sectors and services from 7 to 15.

[4]Please see moredetails regarding NIS2 in https://ec.europa.eu/digital-single-market/en/news/revised-directive-security-network-and-information-systems-nis2

With regards to the Banking and Financial Sector, NIS directive requires that member states that are not within the Banking Union to be regulated and supervised by a relevant banking authority. Such is the case for Norway, having Finans Tisynet as the Financial Authority with the responsibility to enforce seucirty measures and standards as required by within the European Union.

2.1.3 The NIS Trasposition

2.1.4 Review and continuos improvement

The European Commission actively monitors and assesses each of its members states adaptation and implementation of the NIS Directive. The European Commission official website[3] provides a tool and an interactive map to navigate and view each members states current implementation of the strategy, the agencies and authorities involved as well as each Member State's NCSS.

Furthermore, the NIS directive §4 outlines the importance of having all the members of the European Union engages with the issues involving Cyber Security collectively. Having a cross border collaboration and sharing of information are key to defeating a threat that is inherently agnostic to geographical location and legal jurisdiction, NIS §6. European Commission and VIIRA, 2016

The provisions regarding collaboration, sharing of information and close monitoring and assessement of the policies implemented provides the Commission and all Member States a very good foundation to evaluate and improve the NIS Directive.

2.2 Cyber Security Stakeholders in the European Union

There certain requirements described in the NIS that every member states must comply with. Amongst are the requirement to establist certain egancies to manange and monitor the directives and strategies and to enforce the policies derived from it. One such agency is the establishment of National Computer Security Incident Response Team (CSIRT)

Follow-up - !!!
Outline the entities, their roles and responsibilities with regards to the OES, CIIP and the Finance sector:

- NIS Cooperation Group (https://ec.europa.eu/digital-single-market/en/nis-cooperation-group)
- ENISA
- The European System of Financial Supervision - Sectore regulation and supervision.
- The European Securities Markets Authority - Direct supoervision of credit-rating agencies and trade repositories

How lex specialis applies with NIS and Norways National laws and regulations.

Follow-up - !!!
Remember to put link to section "Legislation process" Describe the difference between Decision, Directive and Regulation

Online archive of European Union Law: https://eur-lex.europa.eu/homepage.html?locale=en

[3] https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive

2.3 The Norwegian National Cyber Security Strategy

Norways approach to its NCSS is largely in compliance with the NIS Directive. Although Norway is not directly mandated to adhere to the NIS Directive, aligning and being compliant with EU's regulations and policies is both sensible and benefitial.

Finance sector regulations, Communications and Privacy laws are a couple of example that benefits Norway by allowing for free movement of goods, persons, services and capital with otherEEA Member States. Compliance and with the mentioned laws and regulation makes it much simplier by implmenting NCSS in accordance with the NIS directive.

2.4 Establishing Norways NCSS

Follow-up - !!!
Outline the processes and committes involved establishing the strategy:

The Ministry of Justice and Public Security is responsible for the preservation and development of basic guarantees of the rule of law.

Definition NOU = Norges offentlige utredninger by https://snl.no/Norges_offentlige_utredninger_(NOU) Norges Store Leksikon

The Process - A government or any of its departments recognizes a problem-area, an issue, and is set on a task to remediate for the country's electorate and society at large.

- The department entity then establishes a committee, a council, whom are designated a mandate and an objective to work on the case.

- The committee can be comprised of many different entities. Both public, private or ideal organizations. Researchers, subject matter experts or anyone who may provide valuable contributution to the endevour.

- The committee is tasked to investigate and report their findings back to the responsible/sponsor government department.

- The findings are subject further for debate and political process by the departments, public or private organizations or other stakeholders and interested parties.

- The process will decide if there is merit for the findings to be submitted and presented to the parliament for legislative process. The findings are presented as a white paper, a Stortingsmelding, which will be a end note

Stortingsmelding/White Paper

https://www.regjeringen.no/no/dep/jd/org/styre-rad-og-utval/innstillinger/innstillinger-fra-utvalg/innstillinger-levert-i-20
IKT-sikkerhetsutvalget/id2570775/

IKT-sikkerhetsutvalget Skattedirektør Hans Christian Holte, Oslo (leder) Direktør - Cybersikkerhet Terje Wold, Tromsø Administrerende direktør Håkon Grimstad, Trondheim Head of Information Security Lillian Røstad, Nesodden Direktør internett og nye medier Torgeir A. Waterhouse, Oslo Forskningsleder Marie Moe, Trondheim Professor Lee A. Bygrave, Oslo Lagdommer Therese Steen, Oslo

The Committee established a reference group and consult with stakeholders from different ministries and departments: - Minister of Justice and Public Security - Monica Mæland (Conservative Party) - Ministry of Defence - Frank Bakke-

Jensen (Conservative Party) - Ministry of Local Government and Modernisation - Nikolai Astrup (Conservative Party) Linda Hofstad Helleland (Conservative Party) - Ministry of Transport - Knut Arild Hareide (Christian Democratic Party) - Ministry of Trade, Industry and Fisheries - Iselin Nybø (Liberal Party) Odd Emil Ingebrigtsen (Conservative Party) - Office of the Prime Minister - Erna Solberg (Conservative Party) - Nasjonalt cybersikkerhetssenter

The committees effort has its foundation from: - https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/ NOU 2015: 13 Digital sårbarhet – sikkert samfunn ble våre digitale sårbarheter kartlagt - https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/ Meld]]. St. 10 (2016–2017) om samfunnssikkerhet - ttps://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/ Meld]]. St. 38 (2016–2017) IKT-sikkerhet — Et felles ansvar

The committee must adhere to: - Prop. 153 L (2016 – 2017) https://www.regjeringen.no/no/dokumenter/prop.-153-l-2016-2017/id2556988/ Lov om nasjonal sikkerhet]] – Proposal from the Ministry of Defense based on a NOU from 2016: 19 - Personvernregelverk / Privacy law - GDPR

The committee's deliverable was a white paper https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/ NOU 2018: 14 IKT-sikkerhet i alle ledd — Organisering og regulering av nasjonal IKT-sikkerhet, white paper addressing 3 key issues (released on 2018-12-03): 1) Applicability and aptness 2) Organization and coordination 3) According to findings in 1 and 2, establish and enforce effective regulations following EU NIS Directive.

The https://www.regjeringen.no/no/aktuelt/utvalg-foreslar-flere-tiltak-for-en-sterkere-nasjonal-ikt-sikkerhet/id2621146/ press release from IKT Committee concludes: Norway's Information and Communication Technology Security was inadequately legislated and regulated.

The report outlined the need for a law to be passed for Governmental Procurement and acquisitions where ICT Security is relevant.

New laws and regulation must be establish to regulate ICT Security where Public Services and Critial Information and Communication Infrastructure can be impacted.

A centralized national ICT Security organization is proposed to be established. An organization who can operate horizontally between state departments, agencies and private entities. Who's responsibility is to manage and coordinate Norway's ICT Security effort.

2.4.1 Norways Objectives

Follow-up - !!!
Expand and elaborate on:

National Cyber Security Strategy

Vision In Norway, it is safe to use digital services. Private individuals and companies have confidence in national security, and trust that the welfare and democratic rights of the individual are being safeguarded in a digitalised society.

Strategic Goals 1. Norwegian companies digitalise in a secure and trustworthy manner, and are able to protect themselves against cyber incidents

2. Critical societal functions are supported by a robust and reliable digital infrastructure

3. Improved cyber security competence is aligned with the needs of society

4. Society has improved ability to detect and handle cyber attacks

5. The police have strengthened their ability to prevent and combat cyber crime

2.4.2 Norways Objectives

Follow-up - !!!
Refer to the BDO analysis that compares Norways strategy with EU's Directive. Ref https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/sved/1.pdf. An Analysis performed by BDO which cover the objective of this project.

Instead of redoing and performing the anaylisis again. Refer to the findings and recommendation from the BDO analysis in combination with the EU's own NIS analysis. And perform a meta anaylisis on both.

3 Conclusion

Norway is actually 100% aligned with the European NIS Directive. However, there is little evidence that Norway has identified its OES according to EU's guideline.

Follow-up - !!!
Outline the complexities navigaating the different documents and legislations in the EU and Norway.

There are many stakeholders, authorities and agencies, that regulates and sets policies. Often with over lapping responsibilities and objectives. Making passing policies and implmenting policies complicated.

Many Member states must adhere to and align both National and EU NIS Directive when establishing or revising their NCSS. Again, adding to complexity and GAPS.

A mix and differing definitions and terminologies are bing used and are not always aligned with each other. Making translation of policies tricker. There is a lack of formal and standardised definitons on most cases.

A Appendix

This is the appendix

B Bibliography

References

European Commission. (2017). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL CORRIGENDUM* (tech. rep.). European Commission. Brussels. https://ec.europa.eu/info/law/better-regulation/have-your-say%7B%5C_%7Den

European Commission, & VIIRA, T. (2016). NIS Directive. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148%7B%5C&%7Dfrom=EN%20https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L%7B%5C_%7D.2016.194.01.0001.01.ENG%7B%5C&%7Dtoc=OJ:L:2016:194:TOC%20https://ec.europa.eu/digital-single-market/en/directive-securi

Glossary

CSIRT Computer Security Incident Response Team. 7

DSP Digital Service Providers. 5

EEA European Economic Area. 8

European Single Market A trading agreement between 27 European member states, 3 member states via the European Economic Area, EØS, agreement, and Switzerland via their bilateral trieties with the European Union. The trade agreements key objective is to ensure The "Four Freedoms" as key components for economic growth and stability for all its members. The Single Market includes policy for trade and transactions conducted on the Internet. The European Single Market is also referred to as Internal Market or Common Market.. 4

NCSS Natioan Cyber Security Strategy. 5, 7, 8

NIS The Directive on security of network and information systems. 4

OES Operators of Essential Services. 5, 11