# 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: | 7 |

## 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 accouts 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 Information and Cyber Security.

- 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 part.

## 2.1 The NIS

# 3 Conclusion

Conclusion

This is the conclusion page with a code listing.

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

# A Appendix

This is the appendix

# B Bibliography