Protect Critical Information Infrastructure

Sweden

Sweden is compliant with the NIS Directive and their implementation of the Directive is rated "Transposed". Sweden follows ENISA's Good Practice Guide for National Cyber Security Strategy. However, the Swedish National Cyber Security Strategy does not clearly state any methodology or progress of any activity to identify OES.

Although there are no specific mentions of identified OES, the Swedish strategy shows that there are 2 supervisory Authorities already established as supervisory authorities. These are the Swedish Security Service and the Swedish Armed Forces. These 2 entities have close cooperation with other agencies such as Svenska Kraftnät, Swedish Transport Agency and County Administrative Boards. Together, these agencies and authorities provide the supervision, management and maintenance of essential services.

The Swedish Civil Contingencies Agency (MSB) is the single point of contact with regards to acquiring and sharing security incidents. It is responsible for establishing a number of forums for information sharing, designated as FIDI's. There are FIDI's, or forums, for Telecom, Swedish CERT, Finance, Health and Social Care, Supervisory Control and Data Acquisition, and National Telecommunications Coordination Group. The FIDI's allow for each of the represented sectors who provides essential services to share information and collaborate on Cyber Security issues and incidents.

Denmark

Denmark is compliant with the NIS Directive and their implementation of the Directive is rated "Transposed" and has implemented a decentralized approach. Denmark follows ENISA's Good Practice Guide for National Cyber Security Strategy. Denmark's National Cyber Security Strategy does not clearly state any methodology or progress of any activity to identify OES.

Denmark aims to be a digital frontrunner. The danish government has allocated 1.5 billion DKK for Cyber and Information Security measures over the next few years, shows their commitment to the cause. Denmark's National Cyber Security Strategy has identified sectors it regards as critical and providers of essential services. With 25 specific initiatives and targeted strategies to secure the counties most critical sectors. The Strategy also aims for unified and consolidated Cyber Security approach.

Among the findings and challenges Denmark identifies as security risk are outdated ICT systems within the Central Government. Plans and measures to address this issue is outlined in the National Cyber Security Strategy. Some actions have already been performed to address certain issues and strengthen Cyber Security posture. Among this is the implementation of ISO27001 and other best practices and standards. In addition to monitoring of its information and communication technologies. From the private sector point of view, the Danish Business Advisory Board has conducted its own review and assessment of ICT vulnerabilities. They have developed a method to conduct digital security checks for small and medium-sized businesses.

Other agencies involved with the activities around the Danish Cyber and Information Security Strategy, Center for Cyber Security who manages and maintains the sensor network to detect cyber threats and incidents for authorities and businesses. The Cyber Security Strategy outlines a plan to establish a National Cyber Situation Centre with the responsibility to provide an overview of the National Security situations. Danish Defence Intelligence Service has the responsibility to strengthen its analytical capacity increased. Danish While the Danish Armed Forces aims to increase its capacity to engage with military cyber operations.

Finland

Finland regards itself as an "information society" and as such relies heavily on the Information and Communication Technology and infrastructure which facilitates the digital services for its population. Finland acknowledges that Cyber threat, and disruptions are affecting the ICT infrastructure with ever increasing frequency and severity. And that the Cyber-attacks on the infrastructure has an increasing potential to render a broader section of digital services with considerable to impact to its users.

Vital functions are identified as services and infrastructure provisioning: "management of Government affairs, international activity, Finland's defence capability, internal security, functioning of the economy and infrastructure" to name a few. These vital functions are addressed in Finland's Government resolution on "Security Strategy for Society", from 5th of December 2012. An established and strong collaboration between the public and private sectors is regarded as Finland's key advantage towards a successful implementation of the countries Cyber Security and Strategic goals.

The organization and authorities supporting the strategy is described to take a decentralized approach. Where a Security Committee has an active role in facilitating the cooperation between business communities and organization with the governmental ministries. Along with public administrative offices, both locally and regional. There are 10 strategic guidelines defined in the Cyber Security Strategy. There is however no critical infrastructure specifically targeted by the strategic guidelines. On the other-hand critical infrastructure are implied targets on several of the strategic initiatives.

Iceland

By 2026, Iceland has set its aim to be an "Internet Culture" and has planned to commit 20 million ISK for the initiative. Iceland regards the country's economic prosperity and developments relies heavily on a secure and reliable cyber space. Both as an arena for its citizens to conduct business and consume and provide services in. As such, it is implied that critical services will have to be managed and provided by information and communication infrastructure and thus require to be thoroughly secured.

The Ministry of the Interior mandated a Task Force to establish a National Cyber Security Strategy to protect Iceland's infrastructure. Having the country's "Internet and Information Technology" within its scope. The strategy seeks to enhance its populations Cyber Security posture. Establish an integrated Infrastructure, and a closer cooperation and collaboration between Icelandic and international authorities with regards to Cyber Security. Iceland's Cyber Security strategic goals addresses, albeit without specifically mentioning or targeting, its Critical Information and Communication Technology infrastructure.

A task force will be established to review neighboring Nordic countries Cyber Security Strategies. And to recommend and approach to attain the countries the strategic goals and objectives. It will comprise of The Ministry of the Interior, Head of Department of the Information Society Project, the Office of the National Commissioner of the Icelandic Police, the Post and Telecom Administration, the National CERT, the Ministry of Foreign Affairs and the Data Protection Authority. The implementation of Cyber Security Strategy will be the responsibility of a Cyber Security Forum, comprising of both public officials and entities together with representatives from different private sectors.

UK

The UK regards itself as a modern digital driven society. They have therefore committed 860 million GBP (Although another figure, 1.9 billion GBP, is mentioned in the Executive Summary section 1.14.) in Cyber Security to "Defend, Deter and Develop" a resilient and secure infrastructure to allow its citizens to be "prosperous and confident in the digital world". The improvements and investments targets establishment of "Cyber Innovation Centres".

The UK Government has a plan to have a more active role, both in public and private sectors, in raising the UK's cyber security standards in five years timeframe of the current National Cyber Security Strategy. Power grids, medical technologies and the networks facilitating digital communication are considered vulnerable and will adversely impact large portion of the society. These are Critical National Infrastructures (CNI) and services the National Cyber Security Strategy has identified will require investments for upgrades, modernization and other improvements to be secure.

There are not many specifics on which critical infrastructure will be the target of the Cyber Security efforts. The strategy indicates mandating key agencies and institutions to manages the specifics on the implementation. National Cyber Security Centre (NCSC) is one such agency task with the responsibility and authority to implement the national Cyber Security Strategy. The organization will manage the knowledge, identify and address vulnerabilities.

Estonia

Estonia prides itself to be one the first to recognize the need to promote and implement a National Cyber Security Strategy. It became apparent that a targeted and consolidated effort is required to address and mitigate information and communication technology, and other essential service provider's vulnerabilities, when the country was a target of malicious cyber-attack in 2007.

The Estonian approach to managing and implementing its National Cyber Security Strategy is largely decentralized. Delegating the planning and application of Cyber Security principles to different sectors. The government and the public sector do however mandate some standards and principles to be applied nation-wide. There is also a government cloud solution being developed to guaranty security for its users. In addition to other are state sponsored agencies that provides Cyber Security related services. The likes of State Information System Authority, providing security related information and annual publications. Internal Security Service, Foreign Intelligence Service, helps with studies and analysis on risk and cyber defense exercises.

Estonia's National Cyber Security Strategy addresses specific areas in its critical infrastructure. The strategy promotes the implementation of a national, government issued, digital signature for public and public transactions. The strategy promotes the cryptographic solutions for digital ecosystem and the implementation of "x-road", a government sponsored data exchange layer. The strategy promotes the principles of security and resiliency by design. Like its "no legacy principle", risk-based approach, and a preference for transparent and best-practice solutions for the services and infrastructure the country relies on.

France

France's National Digital Security Strategy began taking shape in early 2010 due to a cyber attack. The Attack exposed France's technical vulnerabilities in their Information and Communication Technologies infrastructure. It also brought forth the acknowledgement the nation's competency in cyber security must be elevated. The latter has prompted for the action to expand the broader populations digital literacy. And the need to foster expertise within the ministries, to properly address cyber security and implement policies for safe and efficient digital transformation.

The National Cyber Security Strategy states its objective to "reinforce the digital security of its critical infrastructure". Where the ultimate goal is to secure its essential operators and economy from intrusions and disruptions. The strategy's do not define what constitutes critical infrastructure and essential services. It does however imply that critical infrastructure facilitates the functioning and prosperity of the society and its citizen. Giving the 5G mobile network having a specific mention.

Cyber Security is addressed in a very top-down, hierarchical manner in France. The Where the government takes and active role to influence and drive the development, and manage the implementation of policies concerning ICT security. They do however acknowledge that the issue of cyber security can only be truly successful if taken as a collective effort, both public and private sectors. As a national commitment and a personal responsibility. There are three communities of stakeholders; the experts and service providers – to provide technologies and implement solutions, the Government and unions– to develop and enforce policies and the responsibility to protect the nations interest in cyber space, the citizen – the responsibility to be knowledgeable of proper use and conduct on the internet, and compliance with policies.

Netherland

Netherland's National Cyber Security Agenda is one of many policies, acts and regulations put forth to address security issues. Several government bodies and authorities have areas of responsibilities that overlaps each other. Which can lead to unclear jurisdictions and boundary of responsibility or result in fragmented situational awareness and uncoordinated resolve. The agenda is therefore designed to be generic, independent of sector or jurisdiction in its scope. And flexible in structure to easily adapt to the latest threat assessment. The agenda also highlights that the Government Coalition has allocated 95 million EUR to address the situation and implement mitigations.

As with most Member States, Netherland has a high utilization of digital services which are integral to the economy and daily functioning of the society in general. Thus, many digital services are deemed essential. And the interconnected infrastructure they run on regarded as critical. Extensive cooperation between the public (government agencies and authorities) and private entities (business, forums, unions and its citizens). And enabling the stakeholders with a high level of awareness, knowledge, and understanding of cyber security, key to successful implementation of the security agenda.

Parts of the funding allocated to address cyber security will be used to invest on staff and ICT for key Governmental agencies. The agenda also targets telecommunication resiliency. Further development of the "Roadmap for Digitally Secure Hardware and Software", for identifying risks and certifying ICT. Establishment of sectoral supervisory bodies. Implementation and exercise of resiliency and crisis plan. And providing alerts and advice on security threats as areas of investments. Many of the measures listed above, although not mentioned explicitly, will help improve essential service and critical infrastructure resiliency and security.

Romania

There is a slight difference on how Romania approaches the matter of Cyber Security. Their National Cyber Security Strategy classifies their infrastructure as two different systems. The designated "Critical Infrastructure" refers to what is utilized by banking, transport, energy and national defence sector. While the "Cyber Infrastructure" is designated to the systems that provisions the country's "Cyberspace". As such the notion of having a "Cyber Security Strategy" pertains, in most cases, to "cyber infrastructure" and not the other. Romania regards that the threats to its critical infrastructure, are due to increasing interdependency between cyber infrastructure and "public utility" critical infrastructure.

The Romanian strategy also states that the responsibility, to implement security measures, resides on all the stakeholders and mutual trust between them. All owners and users of cyber infrastructure are accountable to take the appropriate measures, to secure the infrastructure and to not affect others. Public and private sectors are required to collaborate. Where the key objective is on "exchanging information of threats, vulnerabilities and risk".

The state does otherwise provide policies to address security threats by mandating the application of minimum security requirements according to best practice. By requiring the implementation of national risk management, incident management and increase of resiliency by application of business continuity process. There is also a mandate to develop international cooperation on cyber security. Where the priority is to secure cyber infrastructure supporting national and European infrastructure while maintaining optimal efficiency of available resources.

The Romanian and their Member State counterparts have similar otherwise similar assess

The state as coordinator of cyber security initiatives. Impose regulatory approaches, development of cyber defence.

Develop security culture.

"Establish and implement security profiles and minimum requirements for national cyber infrastructures, relevant in terms of the proper functionality of the critical infrastructures"

"ensure the resilience of cyber infrastructure."

"Prioritization – efforts will focus on securing cyber infrastructure supporting national and European critical infrastructures."

"Dissemination – ensuring the transfer of information, expertise and best practices in order to protect cyber infrastructure."

"Accountability – All owners and users of cyber infrastructure must take the necessary steps to secure their infrastructure and not affect other users."

"Separation of networks – reducing the likelihood of manifestation of cybernetic attacks, specific Internet network on cyber infrastructure that provide vital State functions. Using dedicated networks and separate Internet."

Cyber attacks against the infrastructure supporting public functions of information society services, can disrupt or damage m danger to the national security.

Initiatives and measures:

completing and harmonizing the national legal framework in the field, including setting up and applying minimum security requirements for national cyber infrastructures.

Increasing the resilience level of cyber infrastructure.

National Cyber Security System the general framework of cooperation between private and public entities. Share knowledge, prevention and countering threats. Mutual trust.

Incident management and business continuity, backup and recovery

Cooperation between public and private cyber infrastructure

Cyber Security Operative Council (COSC) (consist of several Government entities) coordinates National Cyber Security System (NSCC)

Ministry for Information Society, coordinates other public authorities not part of COSC

National Response Centra for Cyber Security Incidents (CERTO)

Concludes to implement a national minimum standard of processes and cyber security infrastructure.

Policies will mandate responsible authorities to allocate appropriate funding required to establish address cyber security.

Cyber Security Risk Management.

Norway

Norway approaches the matter of Cyber Security in a decentralized manner. The foundation on which Norway's strategy rest upon are mutual trust and individual accountability. Wherein the authorities provide the guidelines policies and facilitates all stakeholders the means to successfully implement the policies and conduct their business and responsibility. The decentralized approach involves many authorities, private and public entities, and designated stakeholders who are required to collaborate and cooperate on common goals, principles, processes, and procedures.

The overarching coordination and the responsibility of implementing the policies rely on two government entities. The Ministry of Defense who's responsibility is the defense sectors Cyber Security. This includes the element of Cyber Defense, which entails a more active and proactive approach on threats. They do however rely on certain private entities who provides services and the rather heavily on public sectors critical infrastructure. The public sector on the other hand relies on the coordination and policies which the Ministry of Justice and Public Safety is responsible for.

Some of the responsibility towards the public sector involves timely and effectively propagate critical cyber security related information between all stakeholders. Along with the responsibility of establishing the policies, standards, and regulations for the public sector. Which involves the responsibility to acquire relevant input from relevant expertise in relevant fields, and facilitate the collaboration between all parties.

Another aspect of secturing the nations critical infrastructure is

The responsibility

There are many components, layers and moving parts that needs to be addressed for a successful implementations of a National Cyber Security Strategy; International standards and policies, Regional standards and policies, National standards and policies, Sector (private or public) policies, Industry standards, best practices and policies, Technical education, proficiencies and comprehension, Technical solutions and systems implementations, and finally Utilization solutions and enforcement of policies.

Cyber Security is, as with any complex and interconnected systems, only as strong as its weakest link. Requiring all the components, or layers as listed above, to be designed, implemented and function seamlessly together. What is illustrated above is from the point of view in 1 country. The complexity and interconnectedness scales as policies and directives are to be applied on several sovereign states with the requirement for them to align and collaborate.

Assessing how successful Norway is with regards to its Cyber Security will have to be done in three different contexts; how successful it is with regards to actually identifying and mitigating security threats towards is CII, how successful it is implementing its National Security Strategy, and how successful it is with regards to aligning with ENISA's Good Practice guideline and Security Strategy. Let's focus on Norwa'ys Cyber Security Strategy in the context of how it aligns and follows ENISA's Good Practice regarding "Protect Critical Information Infrastructure". Some thoughts and commentary with regards to identifying and mitigating threats and how the strategy is implemented will be injected occasionally.

Norway has taken the decentralized approach towards securing its critical information infrastructure. The strategy recognizes that the expertise and resources required to implement Cyber Security are already within the services providers and each sectors centers of competency (BFI and Nkom). It is therefore the CIIs service providers responsibility to follow its sectors regulations and requirements. These requirements can be wide range of indicators and measurements where Cyber Security is only a subset of auditable components or KPI. It is the sectors supervising authority who's has the responsibility to audit and certify CII with its scope on sector level. While the authority (NSM) can mandate certain KPI levels or crisis management readiness with documented crisis exercises, to assess Norway's security posture on a national level.

There are varying degrees of readiness between sectors and even within each sectors CII service providers. It is also hard to measure how well a sector, the sectors service providers, can cooperate across sectors when outage and disturbance cascades to multiple sectors and escalates in severity. One reason for this is the fragmented audits and validation, where each sector only assesses its own scope of responsibility.

The issues Norway faces is however a common theme throughout the Cyber Security industry. It is due to the inherent complexity and interconnectedness of the digital based economy and society. Norway has otherwise managed to comply with three of four tasks outlined in ENISA's Good Practice Guide for protections of CIIs. In some areas may also exceed the recommendation. Thus is Norway's alignment with ENISA and NIS Directive satisfactory.

in order to have a solid baseline1

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.