"Just tell us what to do"
Regulations and cyber risk appetite in the electric power industry

Silje Aakre
Business School, Nord University, Norway. E-mail: silje.aakre@nord.no

Digitalization in the electric power industry and the society as a whole has led to an update in the industry's regulations for cyber security. Several paragraphs instruct the electric power companies to conduct a risk assessment and implement measures accordingly. This process is the basis for the security level in critical infrastructure. Still, little is known about how this process takes place.

This article shows that cyber regulations and risk assessments can be challenging for the companies. Firstly, the risk perception and risk appetite vary among individuals and institutions, which causes uncertainty regarding which risks are acceptable or not. Secondly, individuals can feel paralyzed by the task as little guidance is provided to help identify and evaluate relevant and acceptable risk. As a result, companies governed by the same regulations can set different limits for acceptable risk and thereby implement very different practices. This article presents empirical data and discuss how and whether clear guidelines can ease this process and improve cyber security.

Keywords: Cyber security, cyber risk, electric power industry, regulations, risk appetite, risk perception, risk acceptance criteria, risk assessment, risk evaluation.

1. Introduction

Electric power is one of the most vital prerequisites for the functioning of modern society. This makes protection of the electric power industry a priority. Electrification is an important factor to achieve goals in the green shift to reduce the need for fossil fuels and decrease CO_2 emissions. Digitalization and thereby efficiency is considered a prerequisite for this change.

The Norwegian electric power industry is regulated by a comprehensive set of laws, regulations and a national regulatory authority. One of the most emphasized regulations is the preparedness regulations, which was recently updated. The main changes are in the field of cyber security and measures, as this field experience technological advances and emerging risks.

Several paragraphs in the regulations instruct the companies to conduct their own risk assessments to serve as a basis for defining acceptable risk and implementing measures. Risk appetite is often treated as a defined reference for when risks are acceptable or unacceptable. The risk appetite can be defined by different actors, such as regulations set by the authorities, or as a part of the internal control system set by the company. There are advantages and disadvantages linked to the use of specific limits or target values for acceptable and unacceptable risk. On the one hand, it can ease decision making and guide practice. On the other hand, it can lead to a shift in focus towards meeting the target value rather than ensuring that the goal of i.e. improved cyber security is met.

A previous study revealed that electric power companies have expressed an evaluation of risk which diverge from the authorities' risk evaluation (Røyksund 2011: 48-50). This indicates that the external regulations might be given a higher or lower priority than intended when adapted into internal routines. This study aims to investigate how electric power companies perceive and respond to changes in cyber risk regulations.

This article consists of five sections. Section two provides a brief review of risk appetite. Section three describes the data collection. In section four, empirical findings are presented. The concluding discussion is presented in section five.

2. Theoretical framework

Risk appetite is what level of risk an organization should accept in order to achieve its objectives, including actions taken to lower risk. Risk appetite is also referred to as risk attitude and risk acceptance. In the management literature, risk appetite is typically seen as a strategic decision for

Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN/DOI: 978-981-14-8593-0

an organization, which can be communicated and applied as a management tool. This can be understood as a formal description of risk, e.g. monetary, as accepted expected loss. (Crouhy, Galai, & Mark, 2006: 88, 157). It is acknowledged that individuals can hold different risk appetites, which might differ from the stated risk appetite of the organization. This can be treated as a question of communicating the organization's risk appetite well enough to guide decisions. (Holmes, 2004: 109-110)

Others argue that a stated organizational risk appetite is problematic on several levels. Risk appetite can vary across individuals and different levels of an organization (Hutter, 2000, in Power, 2004: 19). Further, risk appetite can change because of new information, vary across different aspects of the same risk or even not correspond to any stated appetite (Power, 2004: 19-20). This indicates that an individual's risk appetite will influence their risk perception and thereby influence risk assessments.

Hopkins (2011: 111) argues that when possible, it is important to translate risk management into rule-compliance in hazardous industries. This is because risk management offers little guidance and decision makers need rules to guide their decisions. The electric power industry can be considered hazardous.

Skotnes and Engen (2015: 17) show that the request for prescriptive and detailed regulations will be greater when the problem is perceived to be complex, unpredictable and uncertain. Moreover, they claim that it is difficult to see how introducing more detailed regulations can improve safety.

This indicates that the need for detailed regulations is context dependent.

3. Methodology

The data material consists of interviews, observations and documents.

The author followed a project group consisting of representatives from six different electric power companies led by a project manager from their industry association alliance. External consultants were also engaged in the project group and took part in the meetings and work process. The aim of the project group was to operationalize the external regulations into internal routines and templates, which could be implemented in each company in the industry association.

Data from the project group was gathered on several occasions over six months in 2019. Field notes were taken during workshops, a seminar and regularly status meetings either physical or using a conference tool.

Interview data consists of semi-structured interviews with the project manager, four participants and three external consultants. Prior to each interview, an interview guide with sub-questions custom to the individual's role in the project was prepared. The interview guide was not distributed to the interviewees, instead, they received topics for conversation, typically two to three keywords. Follow-up conversations were conducted with two interviewees for more detailed information.

Observations were also made during an informational meeting held by the authorities concerning the changes in regulations. In addition, observations were made during two preparedness exercises with 20 participating electric power companies.

Secondary data consists of reports and public announcements concerning the updates in the preparedness regulations. This includes a report on the proposed changes with a summary of comments received during the public hearing. The comments include statements from 40 independent actors and the authority's comments.

4. Empirical findings

The empirical findings are based on observations, dialogues and document studies. The findings illustrates the challenges the electric power companies face when required to form internal routines and templates based on their own understanding of the regulations, topics, threat picture and company-specific risk assessments.

4.1 New regulations

January 1st 2019, a new version of the preparedness regulations came into force. The previous version of the regulation was effective for six years only, and the main updates are in the field of cyber security. The regulations are followed by a set of guidelines.

The preparedness regulations comprise paragraphs concerning physical resources and security as well as information and cyber security. The updated version of the preparedness

regulations sets several requirements concerning internal control, documentation, risk assessments, incident management, and technical and administrative procedures, etc. Still, the companies have a high level of freedom in terms of how the requirements are interpreted and met, often based on their own risk assessments.

A public hearing was carried out before the new regulations were finalized. Both electric power companies, industry associations, national authorities and public bodies submitted comments. Electric power companies and industry associations submitted more than half of the comments.

4.2 Risk perception and risk acceptance

The empirical data strongly suggests that the electric power companies perceive cyber security as a complex challenge. During the first meeting, the project group members stated that they lacked fundamental information and a general overview of their company's compliance with the regulations. The group members were unsure about which documents their company already had in place, what the new regulations demanded, whether existing regulations are implemented and work in practice, and which risks to take into considerations. When asked, the individual members estimated that around 30-40 percent of the regulation's demands were in place.

How to communicate cyber security risks and measures to colleagues and management was also raised as a concern. They argued that acceptance is crucial if there is a need to implement new measures or invest in cyber security. Management and different departments within the companies were specifically mentioned. For instance, employees within IT might prioritize the confidentiality of a system as the most important aspect, while employees within operations and administration might prioritize the availability as the most important aspect. This shows that the companies already have experienced different risk perceptions and risk appetites.

The authorities have the possibility to audit the companies' compliance with the regulations. This motivated conversations in the project group regarding what the authorities would consider as the acceptable way to fulfill different requirements, and what would be seen as discrepancies or remarks. Some asked themselves what the people writing the regulations were thinking, e.g. how the authorities define "hub" or "relevant equipment" and intend the companies to fulfill the regulations in practice. The companies tries to take the authority's evaluation of risks into consideration, but find it challenging to determine what the authorities would consider acceptable.

The new regulations gave a more specific distribution of responsibility. The manager e.g., the CEO, the board or top management, holds the overarching responsibility. This means that the manager is responsible for determining acceptable risk on all levels in the company. This might lead to the management choosing a degree of risk in accordance with their risk appetite. Interviews revealed that the top management seldom oversaw the process of adapting external regulations into internal risk assessments and routines. In other words, the person responsible for the risk management is not directly involved in the process, at least seldom in an early phase. It seemed that the most common form of involvement was the IT department etc. asking the manager to allocate funds for investments.

The personnel focusing on adapting the external regulations to internal routines could typically consist of up to five persons in each company. Individuals with this kind of tasks reported having a high degree of autonomy in how to organize their work.

The risk perceptions and risk appetites differs between the authorities and the companies, Moreover, it differs between different departments and among individuals. This makes it challenging to define acceptable risk within a company. The project group members also reported challenges related to finding an effective way to communicate risks within their company.

4.3 Guidance

The regulations are followed by guidelines, with examples on how each paragraph can be fulfilled. Around the time the regulations came into force, a temporarily addition to the guidelines was published. This caused some frustration, as topics revealed as unclear in the hearing were not yet updated and a date for the revised guidelines were not set. The companies expressed that the regulations and guidelines did not provide sufficient information and lacked clear guidelines on how to fulfill the regulations, e.g. through best practice.

Some, especially those who recently had gotten more responsibility within the cyber security domain, almost felt paralyzed by the task ahead because they did not know where to begin.

The regulations were considered comprehensive and the workload substantial. The project group, including external consultants, spent an estimated 800 hours in the project. This covered time spent interpreting and understanding the regulations, identify which documents, templates and routines were needed, and development of these. It is important to emphasize that this represents the workload *before* mapping each company's systems, conducting risk assessments and implementing measures. Even when taking the probability of some overlapping work into account, this is still a substantial workload before the "actual work" can begin.

The previous version of the regulations instructed the companies to perform risk and vulnerability assessments. This is now changed to risk assessments to give the companies freedom in choice of methods to evaluate risks. The use of risk and vulnerability assessments is still widespread. On the one hand, the method uses a framework that easily illustrate acceptable and unacceptable risk as green or red. On the other hand, one specific method might not be suitable in every situation.

An interviewee also problematized the possibility to seek suitable guidance from other actors and sources. It was claimed that security-related information often was not shared because it could be seen as a threat to security if it became known. Furthermore, threats and cyberattacks are heavily underreported, maybe due to stigmatization and limited understanding of the cyber domain versus the physical domain.

5. Concluding discussion

Actors and individuals tend to have different risk appetites and are often uncertain when trying to decide which risks are acceptable or not. This can make individuals feel paralyzed by the task ahead. The methods used to assess risks also vary, and the quality of the risk assessments will depend on the knowledge and understanding of risks.

This indicates that comparable companies can have very different interpretation of risks, the regulations, and acceptable risk. This leads to variation in internal routines and practices. In consequence, the companies might accept "wrong" or "inappropriate" risks. This could go both ways, e.g. more resources are spent than what is purposeful considering the values at risk, or too high risk is accepted.

5.1 Understanding cyber risks

Cyber security is still seen as a relatively new topic by the electric power companies. Compared with the focus on risks in the physical world – it is. The companies seem to be on a more mature level when analyzing physical risks. Some expressed that they lacked knowledge and competence on how to comply with the cyber risk regulations. As a result, actors who lack the knowledge and competence to conduct a reasonable risk assessment might accept too high – or too low – risk.

Sending an email could be considered equivalent to sending a postcard from a foreign country with an unknown postal service in the physical world. You do not know which route it takes, who might read it on the way there, and if it will reach the intended recipient. Depending on the importance and content, this might be an acceptable solution. However, if the postcard or email contain sensitive information, the situation and risk are changed and might be considered unacceptable. In that case, additional security measures, such as encryption, can be applied to reduce the risk to an acceptable level.

The companies expressed clearly that they did not know where to begin in order to meet the requirements in the regulations. The truth is, they will never be finished. One reason is the lack of clear guidelines from the authorities to guide them towards an acceptable cyber risk management. However, the main reason why they will never finish is simply because the world and risks change. The systems, risks, personnel and other factors the risk assessments were based on change over time. When risks are evaluated and measures implemented, it is time to start the process again. Therefore, cyber risk management needs to be seen as a continuous process.

5.2 Rules as legitimacy

The digitalization in the electric power industry has forced the introduction of new technology and related risks. The introduction of the smart meter represent one such example. The implementation of the smart meter in households also introduced new risks of unauthorized access, data

manipulation and in the worst-case scenarios – massive blackouts. Nevertheless, the implementation of the smart meter and thereby related risks was obligatory. The companies had to implement it even if they considered the risk to be unacceptable.

One of the external consultants argued that most IT departments in electric power companies wish the authorities could be stricter because it would make it easier to say no to what was initially considered unacceptable risk. This would apply both to internal and external requests for changes affecting cyber security.

Today, each company has to conduct risk assessments and draw conclusions based on their assessments. As a result, risks can be evaluated differently. E.g., some companies might evaluate cloud services and outsourcing as good and acceptable solutions, while others evaluates the related risks to be unacceptable. A stricter set of regulations could also open up the possibility for the authorities to prevent decisions they find includes unacceptable risk for the electric power supply.

Even though there are disagreements on how cyber security should be improved and the regulations increased their workload, the interviewees were in general positive to regulations concerning cyber security. Some had experienced that the regulations easier legitimized why investments were needed in their company. This made it easier to get approval for increased budgets, which could allow more resources such as software, hardware, training and human resources.

5.3 Who should decide acceptable risk?

In the case discussed in this article, the authorities sets qualitative risk acceptance criteria. It is left to the companies to set quantitative risk acceptance criteria, and the practice seem to vary between companies. Aven (2014: 175-176) is critical towards risk acceptance criteria formulated by industries. He argues that the society as a whole might have a higher willingness to invest in safety to avoid externalities than an industry. Following this argument, the electric power companies might accept risks that are acceptable on the company level, but questionable on the societal level.

Generation, transmission and distribution of electric power is part of the nation's critical infrastructure. The criticality of electric power, suggests that securing the industry is a matter of the national security. Therefore, the state or the authorities should have the opportunity to intervene if they experience (planned) actions that expose the society to a risk that is unacceptable from a societal perspective.

5.4 Closing remark

Findings from both observations, interviews and documents supports that the majority asks for clearer regulations and guidelines, e.g. through the development of best practice. The lack of such creates uncertainty in the electric power companies. The personnel have a large degree of autonomy in how to design internal routines. Some in the project group stated openly that they did not know where to start and felt paralyzed by the task and workload.

The data suggests that cyber risk is perceived as complex, which supports the need for more detailed regulations. Clear regulations and guidelines will most likely minimize the workload spent prior to implementing security measures "finding out what they actually want us to do".

Acknowledgement

I would like to kindly thank Jon Tømmeråas Selvik and Eirik Bjorheim Abrahamsen for your comments and feedback on ideas and draft.

References

Aven, Terje. 2014. *Risk, Surprises and Black Swans*. London: Routledge.

Crouhy, Michel, Dan Galai, and Robert Mark. 2006. *The Essentials of Risk Management*. New York: McGraw-Hill.

Holmes, Andrew. 2004. *Smart Risk*. Padstow: Wiley.

Hopkins, Andrew. 2011. "Risk-Management and Rule-Compliance: Decision-Making in Hazardous Industries." *Safety Science* 49 (2): 110–20. https://doi.org/10.1016/j.ssci.2010.07.014.

Power, Michael. 2004. "The Risk Management of Everything: Rethinking the Politics of Uncertainty." *Demos*, 71.

Røyksund, Marie. 2011. "Informasjonssikkerhet i Kraftforsyningen." Universitetet i Stavanger. http://hdl.handle.net/11250/184580.

Skotnes, Ruth Østgaard, and Ole Andreas Engen. 2015. "Attitudes toward Risk Regulation - Prescriptive or Functional Regulation?" *Safety Science* 77: 10–18. https://doi.org/10.1016/j.ssci.2015.03.008.