LUND UNIVERSITY
SCHOOL OF ECONOMICS AND MANAGEMENT

# Cyber Risk Reporting of Large International Electric Utility Companies

by

Elina Heidenborg

Laura Emilia Lappalainen

May 2021

Bachelor's Programme in International Business

Supervisor: Katja Einola

# Abstract

The purpose of this study is to highlight and dig deeper into an increasingly relevant research area, cyber risk reporting practices. Cyber risk is one of the most significant concerns for businesses worldwide and of specific concern to the energy industry due to the vulnerability and importance of energy companies. A review of risk reporting research reveals the potential value of further longitudinal, industry-specific studies on international companies and that relatively little is known about how businesses in Europe report on cyber risk. Accordingly, this study aims to investigate the cyber risk reporting practices of five large publicly listed international European-based electric utility companies and how their reporting has changed over the last few years. A qualitative content analysis is performed on the annual reports of the five sample companies. The findings indicate that the companies tend to have a positive tone in their cyber risk disclosures, emphasise the mitigation of cyber risk and keep from revealing many details. Change over the years varies between companies, and one company stands out with its highly sparse reporting. The research shows that there seems to be room for improvement in the companies' cyber risk reporting and indicates several potentially interesting avenues for continued research on the topic.

Keywords: cyber risk, risk reporting, electric utilities

Word count: 21 953

# Acknowledgements

As we conclude our thesis, we would like to take the opportunity to thank all the people who have helped us along the way. First of all, we would like to express our gratitude to our thesis advisor Katja Einola for the support, feedback and productive discussions. We would also like to thank Garo Harwood for always quickly answering our questions about academic writing. Furthermore, we would like to acknowledge our appreciation for all the teachers and classmates contributing to a great three years in the International Business bachelor programme at LUSEM. Lastly, it would have not been possible to reach this stage without the support of our families and friends.

# Table of Contents

# List of Tables

# List of Figures

# 1 Introduction

## 1.1 Background

### 1.1.1 Risk Reporting

Following several infamous cases of business and accounting failures at large companies during the start of the 2000s and the financial crisis of 2008, corporate transparency and risk disclosure has pulled a significant amount of attention (Onoja & Agada, 2015; Mazumder & Hossain, 2018). The credibility hits have had investors looking for increased transparency and risk disclosure to facilitate better investment decisions (Onoja & Agada, 2015; Mazumder & Hossain, 2018). Risk disclosure has the potential to reduce information asymmetry between internal and external stakeholders, facilitate stakeholder trust for the company management (Onoja & Agada, 2015), foster a positive perception of the company management and assist in improving a company's reputation (Mazumder & Hossain, 2018). Despite these advantages, the fear of negatively affecting the share price with risk transparency (Mazumder & Hossain, 2018) and the worry of increasing their vulnerability to competitors or other parties looking to gain from the using the information against the firm has served as obstacles against increased risk disclosure (Onoja & Agada, 2015).

As a result of the events at the start of the last two decades, risk disclosure has become increasingly regulated (United Nations, 2017) and the scope of corporate reporting has expanded to include more non-financial information, a logical step as high level management consider this type of information vital to long-term firm performance (Haller, Link & Groß, 2017). Investors and company stakeholders are no longer satisfied with only financial information (Ghio & Verona, 2020) and to fully be able to assess company performance stakeholders need non-financial information as well as financial information (Ştefănescu, Tiron-Tudor & Moise, 2021). Examples of non-financial information include environmental, social and governance (ESG) reporting (Ştefănescu, Tiron-Tudor & Moise, 2021), and non-financial risks are often related to these exact matters (Veltri, 2020).

An example of recent legislation regarding corporate reporting is the EU Directive 2014/95/EU, which introduced new requirements for non-financial reporting for large firms in the EU member states (European Commission, n.d.). The content of annual reports has shifted to include more qualitative information in combination with the traditional quantitative information (Onoja & Agada, 2015). In other words, quantitative and financial information is no longer sufficient when it comes to corporate reporting.

A good understanding of risk disclosure requires a proper definition of the concept. For this thesis the definition presented by Linsley and Shrives (2006, p. 389) has been adopted:

> "in defining risk for this study disclosures have been judged to be risk disclosures if the reader is informed of any opportunity or prospect, or of any hazard, danger, harm, threat or exposure, that has already impacted upon the company or may impact upon the company in the future or of the management of any such opportunity, prospect, hazard, harm, threat or exposure".

The definition is motivated due to its alignment with a widespread understanding of risk (Linsley & Shrives, 2006).

'Risk disclosure' and 'risk reporting' are often used interchangeably (Veltri, 2020), but the reporting and disclosure are not seen as synonyms by all (Dumay, 2016; Veltri, 2020). Dumay emphasises the difference between the concepts by defining disclosure as "the revelation of information that was previously secret or unknown" and reporting as "detailed periodic account of a company's activities, financial condition, and prospects that is made available to shareholders and investors" (p. 178). This thesis will treat the concepts synonymously and not emphasise the difference proposed by Dumay (2016).

### 1.1.2 The Increase in Cyber Risk

The world is becoming more interconnected and digital technologies are increasingly becoming part of crucial business infrastructure. The downside to this, for both the world economy and individual businesses, is the increasing cyber risk. Strupczewski (2021, p. 6) notes the lack of consensus regarding the exact meaning of cyber risk and after a literature review proposes a new definition which is the one adopted in this study:

> "Cyber risk is an operational risk associated with performance of activities in the cyberspace, threatening information assets, ICT resources and technological assets, which may cause material damage to tangible and intangible assets of an organisation, business interruption or reputational harm. The term 'cyber risk' also includes physical threats to the ICT re-sources within organisation."

The Allianz Risk Barometer by Allianz Global Corporate & Specialty (AGCS) identifies cyber incidents as the third biggest corporate risk for 2021 (AGCS, n.d.). The insights are based on survey data from 2700 risk management experts from 92 countries. Cyber incidents have remained in the top three risks identified by the barometer between 2016 and 2020. Cyber related risks also ranked highly in the 2019 Executive Opinion Survey of the World Economic Forum, Marsh Microsoft 2019 Global Cyber Risk Perception Survey and Deloitte's 2017 Cyber Reporting Survey (World Economic Forum, 2019; Microsoft, 2019; Deloitte, 2017). The increasing cyber risk has also drawn investor attention and is ranked as a top threat to portfolio companies' strategic success by institutional investors (EY, 2020).

The possible effects of cyber incidents for companies are numerous. Eling and Schnell (2016) as well as Radu and Smaili (2021) write about financial losses, damaged reputation and interruptions to operations. Spanos and Angelis's (2016) literature review about the relationship between stock prices and information security incidents concludes that such occurrences have a negative impact on the market value of the company. Deloitte's global report (2016) goes

deeper and estimates in its scenario that the known impacts account for less than 5% of all costs, and that financial damage accrues over several years.

There are several varying estimates of the costs of cyber incidents. For example, Dreyer, Jones, Klima, Oberholtzer, Strong, Welburn and Winkelman (2018) tested three different models, and, according to these, the annual global cost of the impact of cyber incidents, including direct costs and systemic costs arising from the indirect impact on the affected company's or industry's suppliers, is between $799 billion and $22.5 trillion (1.1% and 32.4% of global GDP, respectively). In general, several calculations imply that the cost of cyber risk is well above $100 billion annually, although estimates use different definitions of cyber risk and ways to calculate the cost (Eling & Schnell, 2016). The difficulties in assessing the financial impacts on a global scale as well as for individual companies stem from the fact that some of the costs are hidden and more long-term.

### 1.1.3 Previous Research on Cyber Risk Reporting

Given the growing significance of cybersecurity, cyber risk disclosure is gaining research attention. While most studies concern a mix of different methods and observations, three main themes have emerged - companies' reporting practices, the determinants of reporting, and the effects on the stock market. Only the most relevant studies are introduced here, and a more thorough discussion of these themes and related literature is presented in Section 2.2.

Although the cyber risk reporting practices of some top companies in different stock listings in the US, the UK and Canada have been examined (EY, 2020; Deloitte, 2017; and CPA Canada & EY, 2020, respectively), there is a scant number of recent academic studies. Moreover, a majority of them examine Form 10-Ks, which are annual reports to be filed to the US Securities and Exchange Commission (SEC) following specific US requirements (Investor.gov, n.d.). The most germane studies for this thesis are arguably those of Gao, Calderon and Tang (2020), Héroux and Fortin (2020), Pooser, Browne and Arkhangelska (2018) and Skinner (2019).

Apart from Héroux and Fortin (2020), the mentioned authors have researched companies listed in the US. In their longitudinal study, Pooser, Browne and Arkhangelska (2018) found that all the US insurance companies examined identified cyber risk in their reporting in 2015, a notable change from 2006. An example of a more content-focused study is that by Skinner (2019). The author reviewed seven critical US bank holding companies' filings between 2016 and 2018 and analyzed what is said about cyber risk and related risk management and preventive investments. The conclusion is that although the US Securities and Exchange Commission (SEC) issued a recommendation for disclosures of cybersecurity risks and related material incidents in 2011, the banks' practices are rather shallow. Likewise, Gao, Calderon and Tang (2020) researched the language and content of the cybersecurity risk disclosures of 112 public US companies. Their findings show that disruptions and loss of confidential data are in focus, and over the years the disclosures have become not only longer but also more difficult to read.

On the other hand, Héreux and Fortin (2020) examined a wide range of filings and reports of 60 large companies listed in the Toronto Stock Exchange. The study goes more in depth than the above-mentioned articles and analyzes the extent, location, and category of cyber-related

disclosures as well as makes comparisons. Of special interest for this thesis are the results concerning the identification, management, and mitigation of cyber risk. The conclusions illustrate that practices vary between not only industries but also companies, and improvements could be made.

### 1.1.4 Problematization

Haapamäki and Sihvonen (2019) emphasize in their recent review of cybersecurity research in accounting that future research areas include "what kind of information firms and organizations disclose" (p. 831). Indeed, Sections 1.1.3 and 2.2 indicate that research on cyber risk disclosure practices remains limited despite its importance. Most research published in English concerns companies listed in the US and following the US Securities and Exchange Commission's guidelines. This may possibly be explained by the fact that cyber risk disclosure has been regulated there since 2011, which makes such analyses easier. Furthermore, specific industries have not received detailed attention apart from banking and insurance, and to the knowledge of the authors of this thesis, little is known about cyber risk reporting practices across countries. Regarding risk disclosure research in general, there is a need for a more meaning-oriented approach and scrutinies of specific sectors or industries (Mazumder & Hossain, 2018). Khandelwal, Kumar, Verma and Singh (2019) write that longitudinal risk reporting research is more valuable and that existing studies tend to consider single countries. The latter observation is supported by Elshandidy, Shrives, Bamber and Abraham (2018). All this indicates that longitudinal, sector-specific, cross-country research on cyber risk reporting practices is warranted.

This thesis is a step towards fulfilling that gap by providing insights into cyber risk reporting within the energy sector, more specifically electric utilities. Figure 1.1 illustrates the three main components of the research topic. The choice of sector can be explained by its criticality and riskiness. Energy is listed by the EECSP-Expert Group (2017) as one of the vital infrastructures facilitating a working society. However, the industry is volatile and apt to suffer from the impacts of politics and financial crises, which makes energy companies a highly risky investment (Wei, Li, Zhu, Sun & Li, 2019). One of the sub sectors within the energy industry is electric utilities, which is the focus of this thesis to limit the sample and gain a comprehensive picture of the risk reporting practices of relatively comparable companies.

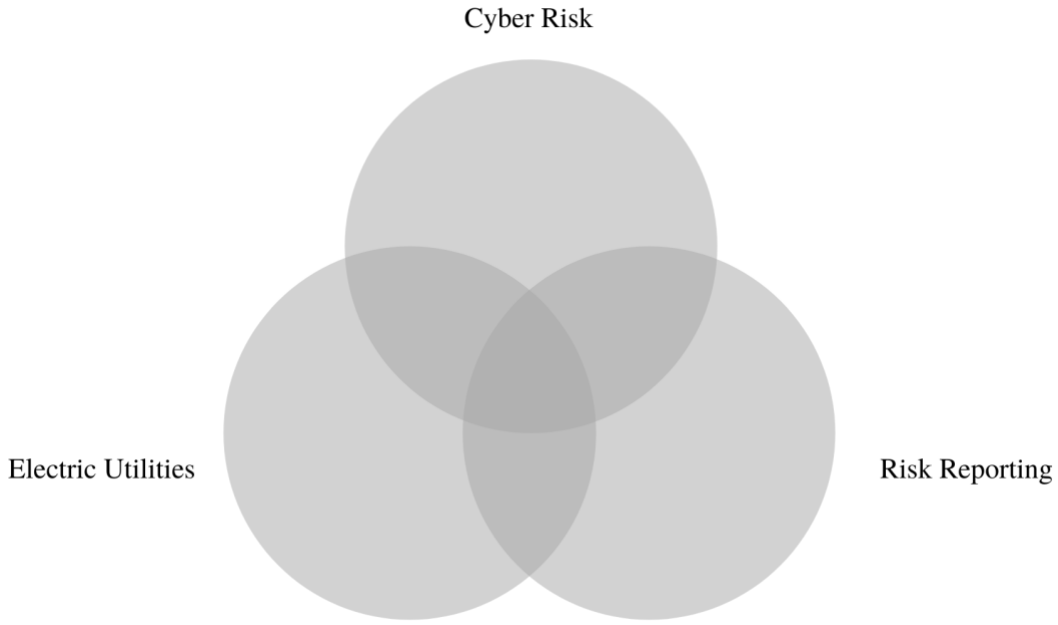


*Figure 1.1 Venn Diagram of the Research Topic*

Concerning cyber risks in particular, Bailey, Maruyama and Wallace (2020) remark that "electric-power and gas companies are especially vulnerable to contemporary cyberthreats" (n.p.). They list three attributes to explain their view. First, there is a recent rise in attacks on the sector by different actors both representing nation-states which are furthering governmental agendas, and those looking out for their own interests. Secondly, the sector is characterized by complex operations, both geographically and organizationally, as well as the often weakly coordinated cyber defence. Finally, mutually reliant cyber and physical infrastructure features in most companies' operations. These remarks are likewise evident in the report by the EECSP-Expert Group (2017).

One example of the realization of a cyber risk within the electric utility sector is the cyber attack on the Ukranian power grid in 2015 (E-ISAC & SANS, 2016) and then again in 2016 (BBC, 2017). The 2015 attack resulted in about 225 000 customers of the affected three companies losing power for hours and was "the first publicly acknowledged incidents to result in power outages" (E-ISAC & SANS, 2016, p. vi). The incidents in 2015 were blamed on Russian security services (BBC, 2017; E-ISAC & SANS, 2016). Ukraine was later the target of a similar attack in 2016, and while no public blame has been placed on Russia, links between the two attacks have been suggested (BBC, 2017).

As can now be stated, cyber risk is an increasingly relevant issue in the energy and the electric utility industry. Nonetheless, such information can be seen as highly sensitive and therefore companies may be reluctant to reveal too much. All this makes it intriguing to examine what companies actually report on it.

Despite these critical issues, little attention has been paid to risk disclosures in the energy industry. The existing analyses of general reporting practices concern mostly issues related to climate change and sustainability (for recent examples, see Chiu, Zhang, Li, Wei, Xu & Chai, 2020; Raquiba & Ishak, 2019; Talbot & Boiral, 2019). Electric utility companies have been investigated from similar perspectives (for instance, Slacik & Greiling, 2020; Traxler & Greiling, 2019). Accordingly, a knowledge gap about risk reporting within the industry and the specific sector remains.

## 1.2 Aim and Objectives

The aim of this thesis is to investigate the cyber risk reporting practices in five large publicly listed international European-based electric utility companies and how they have changed over the last few years. The study is meant to increase understanding of how cyber risk is reported on in an industry specifically vulnerable to cyber risk. To achieve this aim the thesis has several objectives.

- *The first objective* of the thesis is to analyze the cyber risk reporting of five companies in the electric utility industry in 2017, 2018 and 2019.

- *The second objective* is to analyze the development of the companies' cyber risk reporting practices by examining the change in the cyber risk reporting practices over time.

- *The third objective* is to do a cross-case analysis, examine the cyber risk reporting practices of the sample companies as a group and highlight similarities and differences.

## 1.3 Research Purpose

The purpose of this study is to highlight and dig deeper into an increasingly relevant research area, cyber risk reporting practices. The ongoing digitalisation of business infrastructure has allowed companies to leverage new digital technologies to improve their daily operations. With the many advantages there also comes an increased exposure to cyber risk, the significance of which was outlined in Section 1.1.2 where both specific consequences and overall costs of cyber incidents were discussed. Cyber risk management may therefore be of significant interest to company stakeholders and the current research on cyber risk reporting research still leaves several significant questions to investigate.

The dearth of industry specific and longitudinal studies has led to the design of the study presented in this thesis: an investigation of the cyber risk reporting practices amongst large international European-based electric utility companies over three years. The industry was deemed as specifically interesting due to the criticality of smooth operations as outlined in Section 1.1.4 and the sector's vulnerability to cyber incidents. Large and international

companies furthermore generally have more complex operations, another factor which should increase the companies' vulnerability to cyber incidents. As noted by Verizon's data breach report, large companies are also targeted to a higher degree than small companies (Verizon, 2020).

The growing focus and attention drawn to non-financial and qualitative corporate reporting during the last few decades and the continued digitalisation has fueled a need for more knowledge in this area. Providing a closer examination of cyber risk reporting practices amongst large energy companies could be of interest for other researchers and academics as well as policymakers looking to influence the development of risk reporting in a certain direction. This thesis further emphasises the development of corporate reporting to managers.

Accordingly, the research questions to be addressed are:

- What and how do large international publicly listed European-based electric utility companies report on cyber risk in 2017, 2018 and 2019?

- How has the companies' cyber risk reporting changed during these three years?

## 1.4 Delimitations

This thesis limits the examination of cyber risk reporting practices to the large publicly traded companies within the electric utility sector. The five companies chosen have their home country in Europe, and they also operate internationally. These companies' 2017, 2018 and 2019 annual reports are examined for cyber risk-related disclosures through qualitative content analysis. The data collection, described in detail in Section 3.3, focuses on the risk sections of the reports examined and is also performed with the use of a list of keywords, potentially allowing some risk disclosures in the reports to go unnoticed. Furthermore, the theoretical perspective is limited to proprietary cost theory, institutional theory, the risk disclosure quality framework by Abraham and Shrives (2014) and the reviewed previous research on (cyber) risk reporting.

## 1.5 Outline of the Thesis

**Chapter 2** discusses previous risk reporting and cyber risk reporting research, relevant legislative aspects, and the framework utilized for developing the initial categories for coding.

**Chapter 3** focuses on methodological issues related to the abductive research approach and design, data collection, analysis, validity and reliability, and limitations.

**Chapter 4** views, analyzes and discusses the data regarding the chosen companies' cyber risk reporting practices.

**Chapter 5** concludes this thesis with final remarks and implications.

# 2 Literature Review

## 2.1 Risk Reporting

The purpose of corporate reporting and risk reporting is well established. Transparency regarding corporate risks works to reduce information asymmetry and provide investors with the tools to make informed investment decisions (Ghio & Verona, 2020). Stakeholders overall can use the information to get an idea of the performance and future of a company (Veltri, 2020). Beyond the benefits to external stakeholders there are also significant incentives for corporate management to better their disclosure (Graham, Harvey & Rajgopal, 2005). A survey and interviews with financial executives revealed that main reasons for corporate disclosure were the following: "(i) to promote a reputation for transparent reporting; (ii) to reduce the information risk assigned to the firm's stock; and (iii) to address the deficiencies of mandatory reporting." (Graham, Harvey & Rajgopal, 2005, p. 38). Significant sources of reluctance to voluntary disclosure revealed by the same study were the fear of setting a disclosure standard which would not be sustainable long-term and revealing proprietary information to rivals.

Following a review of the research on the topic of risk reporting a few significant themes emerge. Firstly, there has been a clear change in the nature of risk reporting, and corporate reporting in general, in the last few decades as the scope of corporate reporting has expanded to include more non-financial information. Secondly, there has been a wide variety of theories used to investigate and explain risk reporting practices. Thirdly, there has been varying, and at times contradictory, results presented in regards to risk reporting determinants and generally unfavourable assessments of the quality of risk reporting. Finally, a brief discussion of state ownership's effect on risk reporting is presented to provide context for the sample companies in this study. Figure 2.1 provides an overview of the discussion presented in this section.


*Figure 2.1 An Overview of Corporate Risk Reporting Research Discussed in Section 2.1*

### 2.1.1 The Development of Corporate Reporting and Risk Reporting

In the book The Evolution of Corporate Disclosure by Ghio and Verona (2020), the authors note the growing relevance of corporate reporting and take a closer look at its changing nature. The traditional way of reporting and emphasizing solely financial information is no longer sufficient to demanding stakeholders, who are increasingly interested in a broader set of information (Ghio & Verona, 2020). In line with this, Veltri discusses the emphasis on non-financial information (NFI) and that risk disclosure "are among the most important type of NFI valued by investors" (2020, n.p.).

This change in focus regarding corporate reporting is often attributed to the rocky period at the start of the 2000s when corporate scandals and the financial crisis emphasized the need for investors to be able to thoroughly vet their investments (Elshandidy, Shrives, Bamber & Abraham, 2018; Gonidakis, Koutoupis, Tsamis & Agorakis, 2020; Onoja & Agada 2015). Gonidakis et al.'s (2020) study establishes, in line with this, an increase in the quantity of risk reporting in Greek non-financial firms after the financial crisis in 2008. Ghio and Verona (2020) further also attribute the changes to societal sociocultural changes. Veltri (2020) notes that the most often reported non-financial risks are environmental and social risks, environmental risks especially drawing a lot of academic attention. In line with Ghio and Verona's (2020) thinking, this reflects the growing sustainability focus in many countries around the world and supports their assertion that sociocultural changes play a part in shaping corporate reporting.

While the content of corporate risk reporting has and is changing, another significant change regarding corporate reporting is the communication channels used (Ghio & Verona, 2020). Companies are no longer restricted by reporting tools or coverings by analysts and the press but have the option to reach out directly to investors and potential investors through, for example, social media (Ghio & Verona, 2020). Elshandidy et al. (2018) mention that it could be worth pursuing further research regarding risk reporting using other sources than just the traditional annual report. Nonetheless, traditional reporting tools such as annual reports remain significant as their content is developing to become more relevant to the modern investor and other stakeholders, and they commonly serve as source material in risk reporting research. They provide a collective source of information and generally include risk-related aspects, partly due to legal requirements.

As the demands and tastes of stakeholders regarding corporate reporting is shifting there has also been significant changes in legislation regarding the inclusion of non-financial information in corporate reporting. Overall, the legislation regarding risk reporting differs between countries from largely voluntary to strictly required (Mazumder & Hossain, 2018). In Europe, Directive 2013/34/EU of the European Parliament and of the Council, requires disclosure of principal risks for all listed companies, and more recently Directive 2014/95/EU of the European Parliament and of the Council, which there is more information on in Section 2.3, came into effect requiring disclosure of non-financial information for certain companies (Veltri, 2020). This is a clear indication of the rising significance of non-financial risk reporting, as it is not only appreciated by stakeholders but also demanded by law (see Section 2.3 and Appendix A).

### 2.1.2 Theoretical Approaches

There exists a variety of theories which have been used to explain the motivations influencing risk disclosures (Vetri, 2020; Ghio & Verona 2020, Mazumder & Hossain, 2018, Elshandidy et al. 2018; Onoja & Agada, 2015). They can be divided into two main types; firstly, there are a group of theories which explain improved risk reporting, and secondly, there are a few theories which seek to explain a solely symbolic adherence to reporting requirements or manager reluctance in revealing too much through risk disclosure (Mazumder & Hossain, 2018). A few examples of commonly used theories are agency theory and legitimacy theory belonging to the first type, and institutional theory and proprietary cost theory belonging to the second type (Mazumder & Hossain, 2018).

This literature review only goes deeper into two theories explaining risk disclosure due to limited scope and the framework used. The framework and the supporting theories were chosen due to the focus on the weaknesses of current risk reporting. Emphasising this perspective allows the thesis to put the results into an overall context of a topic under development and highlight and pinpoint areas in need of improvement. This increases the relevance of the results for users and practitioners of risk reporting and policymakers looking to improve the quality of risk reporting.

The theories utilized in this study are mainly institutional theory and proprietary cost theory. They are used by Abraham and Shrives (2014) to develop a framework "to evaluate the quality of risk disclosure over time" (p. 104). In other words, the perspective used in this study is multitheoretical. The framework is explained in detail in Section 2.4, and a closer explanation of the underlying theories is now provided.

According to institutional theory, companies deliberately imitate the risk disclosures of other companies due to institutional pressures (Veltri, 2020). The motivation behind this is attributed to the goal of demonstrating risk disclosure at the same level as the industry at large and avoiding the uncertainties regarding more precise firm specific disclosures (Abraham & Shrives, 2014). In the same line of avoiding unnecessary uncertainties regarding the potential costs of disclosure, companies may keep to the same formula and become resistant to change once they have established disclosure routines (Abraham & Shrives, 2014).

According to proprietary cost theory, companies may be unwilling to share risk information or be prone to shape it in a certain way in order to safeguard the company's interest (Veltri, 2020). A significant consideration for managers may be whether the information released will or can be used by third parties against the company and how the risk disclosures will affect future cash flows (Abraham & Shrives, 2014). This could disincentivize risk transparency and lead to a significant difference between internally available risk information and what the company decides to disclose to external stakeholders (Abraham & Shrives, 2014). Another managerial worry regarding risk disclosure this theory sheds light on is the one of litigation costs and that "inexact forward looking risk publication can incite investors to sue the firm" (Onoja & Agada, 2015, p. 3).

The theoretical approach chosen for this study helps explain why companies may be unwilling to pursue risk transparency and why current company risk disclosures may leave something to

be desired despite the trend towards increasing corporate transparency. Institutional theory and proprietary cost theory work well together as they highlight different aspects, and a multitheoretical approach is a suitable choice in a situation like this, when no prevalent theory leads in the field (Abraham & Shrives, 2014). The next section presents a closer look at the determinants and quality of risk disclosures.

### 2.1.3 Determinants and Quality

The determinants of risk disclosure have been examined in multiple studies and Veltri (2020) as well as Mazumder and Hossain (2018) take an overarching view of several studies to consolidate the information and see which determinants are significant. Firm size stands out as a determinant which has been concluded by multiple studies to be positively associated with risk disclosure (Veltri, 2020; Mazumder and Hossain, 2018). One study in particular which draws this conclusion is the one by Linsley and Shrives (2006). A review by Onoja and Agada, however, concludes "that there are no globally accepted determinants of risk disclosure" (2015, p. 6). While the review, like those of Mazumder and Hossain (2018) and Veltri (2020), uncovered multiple studies asserting firm size to be positively associated with risk disclosure, Onoja and Agada (2015) also uncovered studies, like that of Beretta and Bozzolan (2004), which established that there was no association between the two. Onoja and Agada (2015) further point out other potential determinants where research has produced contradictory findings and that the majority of the research on the topic has been focused on developed economies.

In motivating their decision to develop a framework to assess the quality of risk disclosures Abraham and Shrives (2014) note the doubts about the usefulness and quality of risk disclosures. They note that while a general increase in the quantity of risk disclosure has been observed as the practice is developing, significant doubts remain about the quality of the information. Their study emphasized the significance of quality over quantity. According to the authors, other research has similarly argued that assessing corporate disclosure by quality and not only quantity, is important so as not to provide a skewed picture of the corporate disclosures. Mazumder and Hossain's (2018) literature review found that risk disclosures have significant weak points and are generally not very specific which compromises their usefulness. This is in line with earlier research by Linsley and Shrives (2006) where the authors also found risk disclosures lacking in regards to investor needs. Another weak point noted by Mazumder and Hossain (2018) is the shortage of quantifying the risks.

Unsurprisingly, another significant point to consider in regards to risk reporting is legislation. As noted in Section 2.3, risk disclosure legislation varies in between countries. While a study by Adam-Müller and Erkens (2020) on European companies revealed a compliance rate of 62 % on IFRS risk reporting requirements in 2007, legislation has been noted to increase the quantity of risk reporting (Veltri, 2020). This is supported by the study performed by Leopizzi, Iazzi, Venturelli and Principale (2020), the results of which revealed an increase in non-financial risk information disclosure by Italian companies following a change in EU legislation.

### 2.1.4 State-Owned Enterprises (SOEs)

Companies within the energy industry are sometimes characterized by state ownership. That includes some of the companies whose annual reports are analyzed in this study. While a full review of the existing literature on the topic is outside the scope of this thesis, this aspect is worth noticing.

Since SOEs are subject to the scrutiny of a wide variety of stakeholders, they may have more incentives for better disclosure. On a global level, the OECD (2015) has published guidelines regarding the corporate governance of SOEs. One critical aspect of the guidelines is transparency. It is suggested that SOEs should be highly transparent and follow disclosure and accounting standards even when they are not listed on a stock exchange, and specific attention is given to risk reporting. There is also academic research on the reporting practices of SOEs. For example, Nicolo, Zanellato, Manes-Rossi and Tiron-Tudor (2021) find that European SOEs are complying with disclosure standards relatively well and have good risk sections in their integrated reports, arguably to improve their legitimacy. On the other hand, Traxler and Greiling (2019) examine electric utility companies' sustainability reporting and find that while stock exchange listing is positively associated with reporting, state ownership is not. Contrasting findings persist within the research area.

## 2.2 Cyber Risk Reporting

Cyber risk has started to gain attention in risk disclosure and accounting research. Based on the review of the current state of art, it appears that there are a few studies about what and how companies report on cyber risks (Daugherty, 2013; Gao, Calderon & Tang, 2020; Héroux & Forting, 2020; Li, No & Wang, 2018; Morse, Raval & Wingender, 2017; Pooser, Browne and Arkhangelska, 2018; Skinner, 2019). Some academics have also investigated the factors influencing cyber risk disclosure practices (Gao, Calderon & Tang, 2020; Li, No & Wang, 2018; Pooser, Browne & Arkhangelska, 2018), and there are recent, mixed findings about how cyber-related disclosures impact the market value of companies (Berkman, Jona, Lee & Soderstrom, 2018; Kelton & Pennington, 2020; Morse, Raval & Wingender, 2017). Figure 2.2 illustrates the discussion presented in this section.


*Figure 2.2 An Overview of Cyber Risk Reporting Research Discussed in Section 2.2*

Much of this research concentrates on the US, and based on a search of relevant literature in English, there seems to be one related study about companies listed in Canada. The 2011 publication and 2018 update of the widely discussed cybersecurity disclosure guidelines by the US Securities and Exchange Commission could possibly be one reason explaining the country-focus. While the guidance does not imply an obligation, it has had a significant impact on cyber risk reporting. According to the guidelines, companies are encouraged to discuss cybersecurity risks and related matters in their 10-K filings (Gao, Calderon & Tang, 2020). As for Canada, the Canadian Standards Association CSA has published several notices regarding the importance of cybersecurity-related issues in disclosures (Héroux & Fortin, 2020).

### 2.2.1 Reporting Practices

Several researchers have evidenced the increasing recognition of cyber-related issues in companies' risk disclosures. No radical changes occurred immediately after the US Securities and Exchange Commission's 2011 guidance were published, but by 2013 most of the largest US companies reported on cyber risk at least on some level (Daugherty, 2013). Morse, Raval and Wingender (2017) examined the issue from a more limited perspective by scrutinizing the term 'cybersecurity risk', and they still found a gradual but steady increase of the term in 10-K reports. That seems to have become the common practice over the years, at least among US property-casualty insurers as studied by Pooser, Browne and Arkhangelska (2018). Their longitudinal study illustrates that while one out of four companies recognized cyber risk in their 10-K forms in 2006, the percentage increased to one hundred by 2015. Additionally, it is not only the presence versus absence of cybersecurity as a risk factor that has changed. Gao, Calderon and Tang (2020) found that the number of words related to cyber risk in US companies' 10-K filings increased notably from 2007 to 2018.

Related findings have been observed in Canada. Héroux and Fortin (2020) took a broader approach and scrutinized annual information forms, annual and quarterly management's discussion and analysis, and proxy circulars from 2017 and 2018 for matters related to cybersecurity. Their sample consisted of the 60 companies listed in S&P/TSX in the Toronto Stock Exchange in Canada. Out of them, 52 recognized cybersecurity among the risk factors.

Furthermore, it is not only about the identification of cyber risk. Although Héroux and Fortin (2020) analyzed a wide range of filings, they nonetheless noticed that some businesses, albeit a lower number, also consider cyber risk mitigation strategies and responsibilities. Skinner (2019) inspected seven significant US banks and their almost 900 filings to the US Securities and Exchange Commission between 2016 and 2018 for cyber risk related notions, and in addition to recognizing the cyber risk, the banks mentioned how they manage and prevent it. Regarding the potential impacts of cyber risk, research implies that loss of confidential data, operational disruptions, and reputational harms are the most notable issues that distress companies (Gao, Calderon & Tang, 2020; Héroux & Fortin, 2020; Li, No & Wang, 2018).

Despite all this, there is some evidence of the questionable quality of disclosures. In the US, cyber risk recognition was rather broad soon after the publication of the 2011 US Securities and Exchange Commission's guidelines (Daugherty, 2013), and it was similar within the sample of listed firms in Canada that Héroux and Fortin (2020) researched. Skinner (2019) also mentions

that the cyber risk related disclosures are highly general across the banks. Another interesting observation is related to the actual incidents companies have faced. In the US, 27 of the 100 large companies studied by Daugherty (2013) mention no specific events, and the banks analyzed by Skinner (2019) do not report such in their filings. Gao, Calderon and Tang (2020) observed that as little as 3.5% of cybersecurity risk disclosures are connected to incidents. Out of the 60 companies listed in S&P/TSX in Canada, 23% discussed actual cyberattacks in some of their filings (Héroux & Fortin, 2020). A more technical and potentially connected critique is remarked by Gao, Calderon and Tang (2020). With the help of Python, the authors estimated the readability of cyber risk reporting. Although the number of words used had increased between 2007 and 2018, the readability had actually decreased. Furthermore, especially large companies scored low in the authors' sample.

This evidence indicates that there is room for improvement in companies' cybersecurity risk disclosures, at least in the US. Businesses might be cautious in their reporting practices as it could possibly make them seen as more vulnerable in the eyes of stakeholders. This is connected to the discussion in Section 2.1 as well; regarding risk reporting in general, companies might not desire to reveal sensitive information, and studies have found that the quality of risk disclosures could be improved. Despite this, different parties also require information and transparency. Moreover, it is crucial to note that differences exist between companies - there are firms providing excellent information - and that there is some evidence that investors indeed value public companies' current cyber risk reporting practices as discussed later.

### 2.2.2 Determinants

Despite the fact that the extent of companies' cyber risk disclosures varies, it seems that it is on the rise overall. As the empirical evidence illustrates, the US Securities and Exchange Commission's guidelines have had a significant impact on cyber risk disclosure practices. Additionally, the annual number of cyber incidents in the US has been found to be linked to the disclosure levels (Gao, Calderon & Tang, 2020). Neither of these factors are surprising since it is reasonable to assume that recommendations by authorities and increasing global cyber risk make companies more prone to report on related issues. Accordingly, while the research is about the US, the conclusions can potentially be extended to other countries.

Research has also identified other potential factors that affect the level of cyber risk reporting. In the US, the early adopters of cyber risk identification were small, highly leveraged, and growing fast (Pooser, Browne & Arkhangelska, 2018). The authors suggest that these firms are the most likely to suffer from potential incidents - "smaller firms will likely have less capital to withstand a shutdown or major loss; firms with higher leverage are sensitive to changes in their cost of capital and growth firms will be perceptive to risks which could impede future growth" (p. 221). Connected analysis is presented by Li, No and Wang (2018). According to them, prior to the declaration of the US Securities and Exchange Commission's guidance, the presence of cyber risk in disclosures was associated with a high probability for future cyber incidents, but the positive connection disappeared in the post-guideline period. The authors interpretation is that companies who are more likely to suffer from a cyber incident reported on such issues before the guidance was published, and afterwards even those companies that face lower risks have started to disclose cyber risk, making subsequent cyber incidents less probable.

Interestingly, Gao, Calderon and Tang (2020) discovered an association between company size (measured in revenues) and disclosure level. The authors do not contemplate the results more but note that they are in line with other risk reporting research. As noted in Section 2.1.3, there is indeed some evidence of the link between company size and risk reporting. The outcome is intriguing considering the above-discussed findings of Pooser, Browne and Arkhangelska (2018).

Moreover, it appears that there are differences between industries. Gao, Calderon and Tang (2020) identified consumer services, software & services and banking as industries in which companies have lengthy cybersecurity risk disclosures in their 10-K reports. Similarly, Héroux and Fortin (2020) observed that consumer defensive, communication services & technology and financial services sectors discussed cyber risk more than energy or industrials. Also, cybersecurity risk mitigation was the lowest in energy and highest in financial services. Héroux and Fortin (2020) considered various filings and their sample was relatively small - 60 companies listed in Canada - but the results are somewhat related to those of Gao, Calderon and Tang (2020) who examined 112 companies listed in the US. Interestingly, both studies reveal that energy companies disclose relatively little. It is argued that the outcomes can be explained by the use of IT within the sectors (Gao, Calderon & Tang, 2020) but that leaves some room for doubt in light of the discussion presented in this thesis.

The literature introduced here raises intriguing issues that are relevant for this thesis's aim and objectives. How does cyber risk reporting look in Europe? Has it changed over the years due to the increasing relevance of the issue? How is the quality of the reporting of large companies within the energy sector?

### 2.2.3 Effects on the Stock Market

There is some recent evidence that disclosure concerning cybersecurity matters can positively impact the market value of the company. Berkman, Jona, Lee and Soderstrom (2018) create a concept called cybersecurity awareness that considers "both the length of relevant [cybersecurity-related] disclosures as well as the relevance of the language used" (p. 511). The authors' findings show that in the US cybersecurity awareness is positively associated with the market value of the company, yet negative terms are not appreciated. Interestingly, the value is also higher for companies that have experienced a cyber incident, which is potentially due to increased confidence in management's preparation for and prevention of future occurrences. Another intriguing observation is connected to the contagion effect that refers to the negative influence that a cybersecurity incident has on a non-breached company within the same sector as the breached company (Kelton & Pennington, 2020). The authors' results illustrate that reporting on cybersecurity risk management can reduce the negative market reaction caused by the contagion effect.

Despite these confirmations of the positive association between disclosures related to cybersecurity/cyber risk and stock prices, there are contrasting findings. For example, according to Morse, Raval and Wingender (2017), businesses that complemented their filings to the US Securities and Exchange Commission with cyber risk after the publication of the guidelines were not seen in a positive light by investors. Furthermore, the sample was 295 firms,

which gives robustness to the evidence. Such potential negative stock market effects could be one factor contributing to why the current disclosure practices have weaknesses.

### 2.2.4 The Knowledge Frontier

As can now be stated, literature related to cyber risk reporting suffers from some limitations. Firstly, most of current research focuses on companies operating in the US and following the cybersecurity disclosure guidelines issued by the US Securities and Exchange Commission, and thus 10-K reports. One exception to this is the study by Héroux and Fortin (2020) that examines the cyber reporting practices of 60 large companies listed in the Toronto Stock Exchange in Canada. Secondly, the research is largely limited to cross-industry analyses and the financial services sector although it is arguably interesting to examine other industries in a more detailed way. This thesis contributes to fulfilling these knowledge gaps and provides further insights into cyber risk reporting.

## 2.3 Legislation

The sample for this report consists of companies headquartered in Europe and as such the majority of them are subject to EU legislation regarding corporate reporting. The special case worth a closer look is Scotland. While Scotland is part of the UK which voted to leave the EU in 2016, the exit did not actually take place until 2020 (EUR-Lex, 2021) and changes in reporting regulations did not go into effect until 2021 (ICAEW, n.d.). In other words, no matter adjustments to corporate reporting requirements from 2021, the country was still under EU jurisdiction during the years of corporate reporting which are examined in this report. Therefore, when this section provides an overview of relevant regulations regarding corporate risk reporting, Scotland is included in the countries following EU regulations, unless otherwise stated. The below-discussed legislative passages are presented in detail in Appendix A.

Directive 2013/34/EU of the European Parliament and of the Council requires that financial accounts as well as a management report be drawn up for publicly traded companies, it emphasizes that the management report of a company is a crucial part of corporate reporting. According to the Directive, one thing the management report is to include is “a description of the principal risks and uncertainties that it [the company] faces” (Article 19(1)). A few types of financial risks are explicitly mentioned, but it was not until an amendment to the Directive through Directive 2014/95/EU of the European Parliament and of the Council that non-financial risks were explicitly referenced as examples of principal risks which the company should consider when preparing the management report. While non-financial risks could be reported before, the amendment requiring a non-financial statement to be added certainly captured the growing relevance of non-financial factors and increased the weight behind these factors.

The rules stated in Directive 2014/95/EU went into effect in 2018 (CSR Europe, GRI & Accountancy Europe, 2018), and while a detailed explanation of the Directive is beyond the scope of this thesis, a short summary of the points relevant to risk reporting is provided. One

type of company subject to the Directive are large companies trading stock on an exchange in an EU member state (CSR Europe, GRI & Accountancy Europe, 2018), in other words, the large publicly traded companies making up the sample for this study. They are required to report on "non-financial key performance indicators relevant to the business" (p. 8) and, at the very least, report on environmental, social and employee matters, respect for human rights and anti-corruption and bribery matters (CSR Europe, GRI & Accountancy Europe, 2018). This information should include information about "the principal risks related to those matters linked to the group's operations" (CSR Europe, GRI & Accountancy Europe, 2018, p. 8). While cyber risk reporting is not explicitly required by EU legislation, this recent Directive has increased the significance of non-financial risk reporting and if cyber security would be considered central to the business it is reasonable to expect a review of the main cyber risks in the companies' reporting. Both Ghio and Verona (2020) and Veltri (2020) describe the directive as rather flexible when it comes to the content of the disclosures required by companies. The disclosure required largely depends on the companies' own interpretation and view of what is material beyond what is specifically mentioned.

While the directive is in force in the EU, it has not been uniformly adopted in all of the member states since they have certain freedoms in, for example, how to define the companies subject to the directive (CSR Europe, GRI & Accountancy Europe, 2018). Overall, while Directive 2013/34/EU and Directive 2014/95/EU have worked to harmonize the reporting practices in the EU, they have still been implemented with differences across the member states. An examination by CSR Europe, GRI and Accountancy Europe (2018) of the national implementation of Directive 2014/95/EU, though, reveal that all the countries included in this study have adopted the same requirements in regards to non-financial risk disclosure as described above. While they are bound by EU legislation, national accounting bodies also tend to publish reporting guidelines. Germany, for example, is considered to have stricter requirements since the German Accounting Standards Board has published relatively specific reporting regulations (Veltri, 2020), for example demanding that "individual risks must either be ranked by their importance or combined into categories of similar risks" (Deutsches Rechnungslegungs Standards Committee e.V., n.d., n.p.). This said, despite the stricter requirements, they do not explicitly require information on cyber risks.

A review of relevant legislation regarding risk report has revealed it to be an area under development. Recent EU legislation has emphasized the significance for non-financial reporting. Cybersecurity or cyber risks are not, however, one of the obligatory non-financial factors mentioned in Directive 2014/95/EU which companies are required to report on. Therefore, whether a company is required to report on cyber risks depends largely on their own situation and interpretation of the current legislation.

## 2.4 Theoretical Framework

As Abraham and Shrives (2014) remark, it is rarely enough to examine the quantity of risk disclosures. Consequently, they develop an approach for analyzing the risk factor disclosure quality and test it in the study of four companies' reporting. The authors' work builds on the

two theories discussed in Section 2.1.2, namely institutional and proprietary cost theory. Additionally, they consult related academic research, disclosure guidelines and legislation to construct the model. The outcome of Abraham and Shrives' research is three themes and three questions connected to disclosure quality, and these formed the basis for the initial data coding for the analysis of the large electric utility companies' cyber risk reporting in this thesis. The framework developed by Abraham and Shrives and its theoretical basis are illustrated in Figure 2.3.

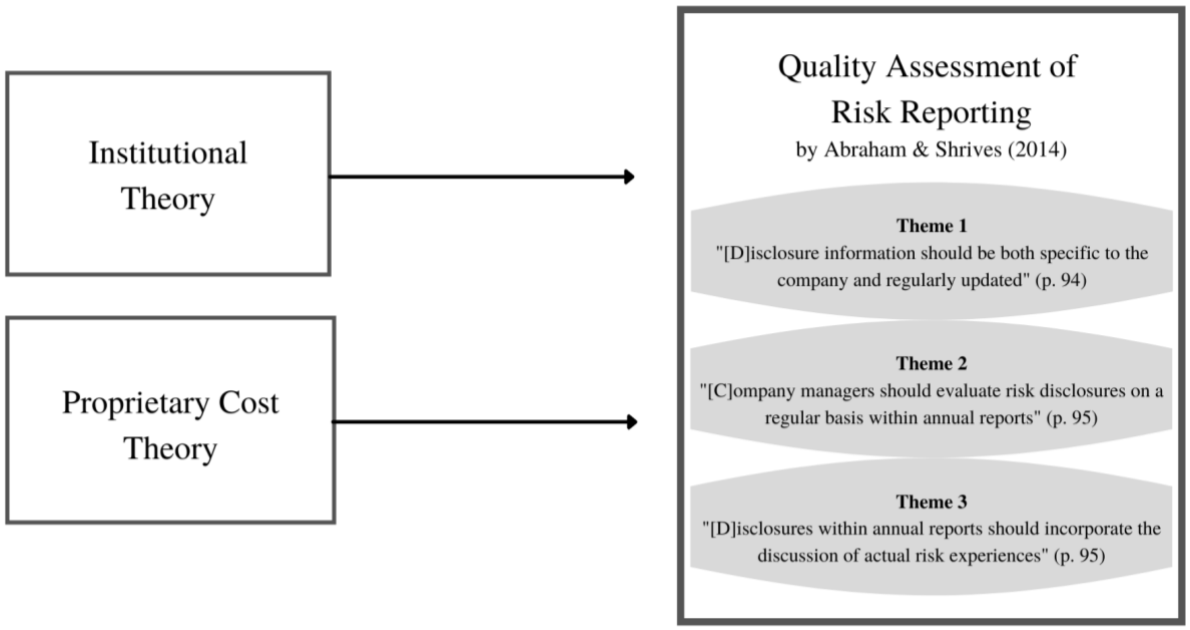


*Figure 2.3 Illustration of Quality Assessment Framework Developed by Abraham and Shrives (2014)*

### 2.4.1 Core Theories

Referring to the earlier discussion, the fundamentals of institutional theory lie in institutional pressures and avoidance of uncertainty regarding more specific disclosures. On the other hand, proprietary cost theory indicates that companies do not desire to reveal too much crucial information. Abraham and Shrives explain their choice of theories from multiple perspectives. In general, the utilization of various theoretical perspectives indicates a more extensive and thus a better approach as the real world is often complex and spans across various theories. Moreover, the authors mention four specific reasons for the two exact theories:

> "First, they provide a way of explaining and understanding the current problematic state of risk reporting. Second, the theories work particularly well both in concert and individually where they can also capture different aspects of risk reporting. Third, the theories can help understand the processes at work which result in limited and general disclosures which bear little or no relation to the risk identification and management processes within organizations. Finally, the mimetic aspect of institutional theory may also be helpful in envisioning a solution to current limitations of risk reporting." (p. 92)

Regarding the second aspect, the review in Section 2.1.2 illustrates that the theories focus on somewhat different considerations. Nevertheless, Abraham and Shrives also emphasize three points that unites the theories. Firstly, general reporting is more likely than company-specific. Secondly, reporting might not describe the true risk management within the business. Thirdly, there is a strong likelihood that change is minimal and reporting becomes standard, unchanged practice. Together with academic, legislative and accounting literature, the authors utilize the two theories to construct themes which are then used to develop the questions for quality assessment.

### 2.4.2 Theme 1

*"[D]isclosure information should be both specific to the company and regularly updated" (p. 94)*

Abraham and Shrives emphasize that guidelines and regulations often ask for companies to describe the principal risks they are facing. According to the authors, reporting can be general, specific to the industry, or specific to the company. The last type is in their argument the most important, since the informativeness of mentioning the general risks the whole industry is facing without any reference to the business in question is low. Indeed, the reviews in Sections 2.1 and 2.2 show that academics often criticise broad and general risk reporting. Regarding risk disclosure updates, it is important to keep the reporting up-to-date. Moreover, Abraham and Shrives write that information related to company-specific risks is inclined to change more than highly general information. Accordingly, updates and revisions are required.

### 2.4.3 Theme 2

*"[C]ompany managers should evaluate risk disclosures on a regular basis within annual reports" (p. 95)*

According to Abraham and Shrives, good risk reporting not only requires but also includes regular managerial evaluations to provide context for the disclosure. The authors emphasize that it can be very informative - for example, it can assure how the risks are relevant for the current business. Such explanations are critical for justifying the unaltered nature of risk disclosure if that is the case. This aspect seems strongly related to the remark about company-specific information and frequent revisions, i.e., theme 1. Correspondingly, the authors have combined these two themes into question 1 and its sub questions which are presented later.

### 2.4.4 Theme 3

*"[D]isclosures within annual reports should incorporate the discussion of actual risk experiences" (p. 95)*

Lastly, Abraham and Shrives state that good-quality reporting is connected to real incidents. The authors divide this theme into two aspects - predictions of actual events and subsequent

discussions. Following their argument, if the risk disclosure is to fulfill its purpose, it should be accurate and foresee risks that indeed materialize. Furthermore, if an incident occurs, that should be reflected in later reporting to increase the reliability of disclosures. The absence of such practice can raise doubts about the connection between risk reporting and actual risk management processes within the company. The authors note that occurrences can and arguably should impact future risk disclosures in some way if something valuable has been learned, as it often is. Again, all this seems to be connected to the specificity of the reporting. This theme leads to two additional questions.

### 2.4.5 Questions for Analyzing Risk Disclosure Quality

Based on these themes, the authors develop three questions and related sub questions for assessing the risk disclosure quality.

*Question 1 (themes 1 and 2):*

"Is risk information specific to the company and are there changes to reported risks in risk factor statements over time?" (p. 95)

- Is the disclosure general or company-specific?
- Has the disclosure changed compared to the previous disclosures?
- Is there an explanation of the relevance of the risk for both the past financial year and the future?
- Is the addition or removal of risk factors explained?

*Question 2 (theme 3):*

"Are significant events identified in prior risk factor statements?" (p. 95)

*Question 3 (theme 3):*

"Are significant observed events discussed in subsequent risk factor statements?" (p. 96)

Although the authors propose that a good-quality risk disclosure considers all these aspects, they also mention that there is no need to be overly descriptive - rather, being concise but informative is more valuable. Furthermore, they note that the three questions might not be the only relevant ones and others might exist, but the framework provides an excellent starting point for evaluating qualitative risk disclosures. While the framework focuses on risk factor disclosure compared to the wider definition of risk disclosure adopted in this thesis, it provides an initial basis for examining the cyber risk reporting of the sample companies and highlights certain dimensions which are interesting to review in qualitative risk disclosures. A more detailed discussion of the utilization of this framework is presented in the next chapter.

## 2.5 Chapter Summary

This chapter outlines the current state of risk reporting research and cyber risk reporting research. The widening scope of corporate reporting and the questionable quality and the determinants of risk reporting are explained. The literature review further illustrates that risk reporting research applies different theories, and the two theories utilized in this thesis, proprietary cost theory and institutional theory, are explained. As for cyber risk reporting, previous research regarding reporting practices, determinants and stock market effects are discussed in this chapter, revealing contradictory findings and a knowledge gap regarding industry-specific studies on non-US companies which this study contributes to fulfilling. Due to the regulated nature of corporate reporting, relevant legislation and the arguably less than strict requirements regarding cyber risk reporting in the EU are presented. Finally, the review further introduces a theoretical framework by Abraham and Shrives (2014) used to assess quality in risk reporting.

# 3 Methodology

## 3.1 Research Approach and Design

For this study an abductive research approach was utilized. Rather than generating theory from empirical data like in induction or testing existing theories like in deduction, an abductive research approach seeks to investigate areas lacking proper theoretical explanations while allowing existing theoretical knowledge to be used as guidelines (Kennedy, 2018). The data steers the study and the researcher is open to a variety of paths going forward. This type of research may result in new interesting hypotheses to test or call to rethink existing theory (Kennedy, 2018). As this study seeks to provide new insights into cyber risk reporting practices in a certain industry, this was deemed the most appropriate approach to follow. Furthermore, the research is exploratory in nature. Following the distinction by Saunders, Lewis and Thornhill (2007), the thesis searches for new insights and explores cyber risk reporting practices in a flexible way instead of studying causal relationships (explanatory research) or merely describing something (descriptive research).

To fulfill the aim and objectives of this thesis, a qualitative research design was chosen. According to Bryman and Bell (2011), "qualitative research can be construed as a research strategy that usually emphasizes words rather than quantification in the collection and analysis of data" (p. 27). As the authors remark, that allows for more flexibility, which can be both a challenge and an opportunity. Since this research attempts to analyze reporting practices and their quality rather than quantify the contents of the risk disclosures, a qualitative strategy was deemed appropriate. Also, as discussed in Section 1.1.4, there is a need for that type of research within the risk reporting field.

More accurately, the method utilized here is qualitative content analysis. That refers to "a searching-out of underlying themes in the materials being analysed" (Bryman & Bell, 2011, p. 560) and is often used for the analysis and interpretation of different types of text (Bryman & Bell, 2011; Julian, 2008; Kuckartz, 2014). It allows for the identification of unconscious and conscious meanings (Julian, 2008). As Kuckartz (2014) writes, qualitative content analysis has evolved from the classical, quantitative content analysis. According to the author, the latter refers to for example word counts and statistics, which also makes deeper analyses difficult since the meaning of the text is not the focus. On the other hand, Kuckartz remarks that qualitative content analysis is more flexible and allows for a real, human understanding and interpretation of communication. He emphasizes that the researcher has a crucial role in that process. Accordingly, in one sense the approach solves some of the issues with quantitative content analysis. Despite this, Kuckartz notes that qualitative and quantitative analyses are not contradictory to each other; they are complements, and sometimes the difference is rather small.

Due to these matters, a method with the characteristics of qualitative content analysis corresponds to the thesis's aim. Bryman and Bell (2011) assert that qualitative content analysis is used relatively little in business research, but that can imply an opportunity for new insights. As discussed in the first two chapters of this thesis, there is a call for more qualitative analyses of risk reporting. Furthermore, within the (risk) reporting research field content analysis in general is common practice (Veltri, 2020).

Additionally, the study has longitudinal elements since several years of reporting are considered. It is appropriate for qualitative content analysis and allows for an examination of a potential change and evolution in reporting practices (Bryman & Bell, 2011; Julian, 2008). Longitudinal research designs are also found valuable in risk disclosure research (see Section 1.1.4).

Possible issues with a qualitative research design include subjectivity, replicability, generalization, and lack of transparency (Bryman & Bell, 2011). Firstly, the authors write that qualitative research implies that the researcher often decides which findings are crucial, which can occur unsystematically. Connected to this, replicability can be a challenge due to the procedures characteristic of qualitative studies. However, because of the nature of the data utilized here and openness regarding the research process, this is less likely to be a complication than the first aspect. Thirdly, Bryman and Bell note that compared to quantitative research, a qualitative approach implies limited generalizability. Nonetheless, the authors write that the aim is rarely to generalize to populations. Such is the case with this thesis as well. There is no attempt to make generalizations about the cyber risk reporting practices - rather, it provides an investigation of how five large publicly traded electric utility companies based in Europe undertake the issue at hand. Lastly, Bryman and Bell argue that qualitative research often lacks transparency. To avoid this, the research process has been explained to a great detail here. Accordingly, the next sections focus on how the sample companies were chosen, how the data was collected, and what steps the data analysis included.

## 3.2 Selection of Companies

To determine which large electric utility companies based in Europe were to be studied, the S&P Global Platts Top 250 list of 2020 was utilized (S&P Global, n.d.a). The ranking includes the top publicly listed energy companies globally, and it is constructed by the companies' "asset worth, revenues, profits and return on invested capital" (S&P Global, n.d.b, n.p.). Furthermore, all the businesses' assets are more than 5.5 billion US dollars.

Since the ranking also categorizes the companies by region and sub-industry, it was straightforward to consider only EMEA businesses within electric utilities. The industries are decided by the Global Industry Classification Standard (S&P Global, n.d.b). Out of these companies, those whose home country is within Europe were chosen. A closer examination into the businesses was also conducted to determine that they have international operations given the aim of this thesis. This procedure resulted in 16 European-based companies. To facilitate a more in-depth analysis, the sample was further narrowed down to the top five companies out of

the 16. The final sample is listed in Table 2.1. The S&P ranking was considered appropriate due to its transparent method and suitability for choosing a sample of large electric utility companies.

*Table 3.1 Selected Companies' Names and Home Countries*

| | |
|---|---|
| Electricité de France SA | France |
| Iberdrola, SA | Spain |
| Enel SpA | Italy |
| SSE plc | Scotland |
| EnBW Energie Baden-Württemberg AG | Germany |

## 3.3 Data Collection Method

To fulfill the aim and objectives, data was collected from the companies' consolidated annual reports, in other words, the reports for the company group. In this thesis, annual reports refer to any consolidated annual publications relating to financial and non-financial statements, governance and sustainability, for example: integrated annual reports, sustainability reports and risk reports. A full list of the reports included as data sources for this thesis is available in Appendix B. The decision to not limit the study to the 'traditional' annual reports was made since company reporting differs and companies may disclose information in differently-named reports.

The research of the relevant literature conducted for this thesis reveals that risk reporting studies often examine annual reports as they are the principal means of companies to discuss such issues in one consolidated place. There are some arguments regarding the increasing number of ways to communicate with stakeholders, but annual reports still have an important role (see Section 2.1). Furthermore, since public companies must create annual accounts and management reports, they provide a relatively comparable data source, and that also guarantees access to data. The public availability adds to the quality of the research presented here through transparency.

To understand the development of cyber risk reporting up until the current state and to ensure the feasibility of the research, the years were limited to 2017, 2018 and 2019. Three consecutive years can potentially illustrate some trends. A decision was made not to include the year 2020 as one company did not have their 2020 reports published early enough for this thesis' purposes. Regarding one of the five companies whose reporting does not follow the calendar years, a similar reasoning, i.e., selecting the three latest financial years for which annual reports are

available, leads to the inclusion of 2017/2018, 2018/2019, and 2019/2020 reports. All the reports were analyzed in a digital form and accessed through the companies' websites.

To collect the cyber risk disclosures, the risk section of the reports was examined for information pertaining specifically to cyber risk and, additionally, the keywords listed in Appendix C were searched with the search function within the whole report. The text passages found were then assessed against the previously mentioned definition of risk disclosure (Section 1.1.1) and if they fit they were then collected for further analysis. These decisions were made since companies are required to disclose principal risks which are most likely within the risk section of the report. However, to ensure that all relevant data was gathered, the keyword search was conducted as sometimes companies discuss highly related issues elsewhere in their reports. The keywords used were adapted from Li, No and Wang (2018) who have constructed a list based on previous research. Companies can utilize a variety of different terms related to cyber risk, and based on the literature review, the keywords utilized seem to cover the crucial concepts and they reflect the definition of cyber risk introduced in Section 1.1.2.

Due to limited scope and time, gaps remain. It is possible that some significant cyber risk information was not found through this method. The keyword list is narrow, but it covers the most important terms and there is a strong belief that the most prominent aspects were captured. Although the cross-country nature of this research could have compromised the comparability of the source material due to national differences in corporate reporting practices, the use of annual publications and not merely traditional annual reports increases the likelihood of a fair view of each company's risk disclosures. Additionally, it is arguably interesting to examine how cyber risk is recognized and communicated in international business. To maximize transparency, these limitations are acknowledged and the details regarding the data collection methods are presented.

## 3.4 Data Analysis

This study analyzed the collected data using qualitative content analysis to investigate how cyber risk disclosures of the sample companies are written. The framework developed by Abraham and Shrives (2014), which is described in Section 2.4, was utilized as a foundation for the initial coding process. The steps taken to perform this analysis are explained below.

### 3.4.1 Qualitative Content Analysis

Qualitative content analysis branched out from quantitative content analysis and allows for a less rigid approach to textual analysis (Williamson, Given & Scifleet, 2018). This type of analysis allows the researcher to look deeper into the meaning of the data than allowed for by solely using quantitative measures and recognizes "that interpretation is required to account for the intricacies of latency and the rhetorical intent a topic attains" (Williamson, Given & Scifleet, 2018, p. 463). In other words, qualitative content analysis is a highly subjective method and the precise process used in this study is described next to enhance transparency.

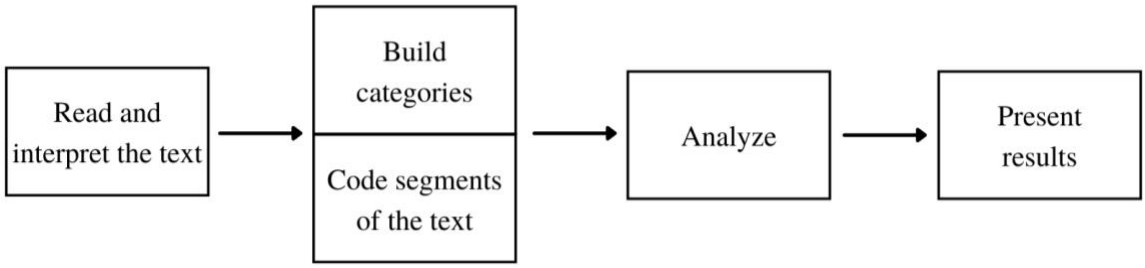


*Figure 3.1 The Process of Qualitative Content Analysis Followed in This Study*

The analysis in this study consisted of the five main activities making up the process of qualitative content analysis as described by Kuckartz (2014) and illustrated in Figure 3.1. The activities are the following: (1) read and interpret the text, (2) build categories, (3) code segments of the text, (4) analyse and (5) present results. Kuckartz emphasizes that these different activities are dependent on each other and that while the order does matter, working with multiple iterations is commonplace to improve the process.

*(1) Read and interpret the text*

The first step of the analysis consisted of reading and interpreting the text passages collected from the companies' annual reports. These were sorted according to company as well as according to year to keep a steady focus on the longitudinal aspect of the analysis. At times the material was also re-read as recommended by Bryman and Bell (2011) to ensure a thorough understanding and an impression of the main points brought up in the text. During the initial work with the text, case summaries were also discussed of every company's risk disclosures. Following the guidelines by Kuckartz (2014), the summaries were simply compressed versions of the disclosures with an emphasis on aspects connected to the research question which assisted the researchers in the next stage of building categories. Re-reading was also repeated several times throughout the entire process of the analysis to see whether new insights or realizations appeared. These were then used to shape the continued analysis.

*(2) Build Categories*

The second step consisted of building categories for the themes and key concepts in the data to capture how and what the companies were disclosing regarding cyber risks. This study used inductive-deductive category construction. This means that the study both used categories derived from the literature review, more specifically the framework constructed by Abraham and Shrives (2014), as well as letting categories emerge from the data collected for this study and then applying them in the analysis. This is a common approach in qualitative content analysis (Kuckartz, 2014). In other words, when the data did not fit with any of the categories derived from the literature review, a new category was created to capture its meaning. This allowed a high level of flexibility in the analysis and for the study to pick up on a wider range of aspects in the analysis than is possible when solely using deductive categories from the literature review.

*(3) Code segments of the text*

The third step consisted of coding the data collected for analysis. This refers to pairing segments of the text to categories (Bryman & Bell, 2011; Kuckartz, 2014). Since this study utilized an inductive-deductive approach to category construction this step was highly interwoven with the previous step. The category construction was not completely finished before the coding started, but categories emerged throughout the process of coding the data. The text was carefully read through and pieces of text were assigned to a certain category. An issue with coding mentioned by Bryman and Bell (2011) is the risk of losing context when plucking parts of the text and assigning them to a category. To avoid losing depth and context in the coding the recommendations of Kuckartz (2014) were followed regarding how to decide the boundaries for a unit of meaning. The guidelines followed were the following: coding was performed of full sentences or full thoughts as Kuckartz emphasizes that the units should be rounded off by semantic boundaries and when pieces of text were pulled from the data for coding, extra text surrounding the main points were at times included so that the passage would still be understood correctly without the context of the rest of the text.

Furthermore, as this study is performed and written by two researchers the method of consensual coding was adopted to improve the quality of the work. This method entails each researcher coding the textual data independently before then coming together and discussing the results and finding a consensus in regards to categories and the coding (Kuckartz, 2014). According to Kuckartz, this method facilitates more exact category definitions and often prompts discussions which may improve the work. Williamson, Given and Scifleet (2018) further argue that involving more than one researcher in the coding process strengthens the reliability of the work as more than one person is involved in deciding appropriate categories and how they are utilized.

*(4) Analyse and (5) Present the results*

Finally, the results of the qualitative content analysis are presented in Chapter 4. The results were sorted according to company in order to emphasize the differences between companies and the changes in each individual company's cyber risk disclosure between 2017 and 2019. The similarities and notable differences between the companies are then highlighted and discussed. The categories and overall themes identified in the risk disclosures are described and discussed in the context of the previously acquired knowledge in the field presented in the literature review.

### 3.4.2 Use of Framework in Analysis

Abraham and Shrives (2014) illustrate the use of their framework developed for assessing the quality of risk disclosures by mainly examining the explicit risk information in annual reports. As previously mentioned, this thesis has a wider data collection and does not limit the study to risk factor disclosures but risk disclosure in general in line with the definition presented in Section 1.1.1. The study does not apply the framework to assess the quality of the disclosures but instead utilizes it as a theoretical foundation highlighting interesting aspects of risk disclosures.

The framework by Abraham and Shrives contributed to the study as it was the source of the predefined categories used in the content analysis for the initial coding. These categories were created from the themes and questions presented in the framework to allow for easy use of the framework in the analysis. As explained in Section 2.4, the three themes in the framework may be evaluated through three questions. The use of these questions in creating categories and in the analysis is explained below and the final themes which resulted from the analysis are listed in Appendix D.

*Question 1. "Is risk information specific to the company and are there changes to reported risks in risk factor statements over time?" (Abraham & Shrives, 2014, p. 95)*

As previously explained (Section 2.4.5), this question is represented more in detail by a few subquestions. These questions led to the creation of various categories which were used in the coding of the text. The first category was *firm-specific information* and the second category was *general information*. In other words, it brought attention to whether the cyber risk disclosures in the companies' annual reports contained information specific to the company or solely a general information true for all companies or for companies in the industry at large. During the course of the analysis, these two categories were condensed into one theme and into two sub themes under the main theme *information scope* as evidenced in Appendix D.

The time aspect highlighted by the question is emphasised in the examinations of annual publications over three years and an attention to potential changes/developments. The final categories created from this question were *past year relevance* (explanation of the relevance of cyber risk for the financial year under review) and *future relevance* (explanation of the relevance of cyber risk for the future). These emphasize the context of the risk disclosure and led to the creation of the main theme *time relevance of the risk*.

*Question 2. "Are significant events identified in prior risk factor statements?" (p. 95) and Question 3. "Are significant observed events discussed in subsequent risk factor statements?" (p. 96)*

These questions led to the creation of the category *cyber incidents*. This emphasizes the presence of information regarding specific events that may have happened to the company in the risk disclosures. While Abraham and Shrives collect data both from annual reports and a news database to identify significant risk events the companies have been through based on high or low stock prices, the scope of this thesis is limited to analysing data collected from annual publications. A deeper investigation of potential cyber incidents through other means would be intriguing, but due to the characteristics of the sample companies, it would take a lot of time. The varying languages of the news covering, the differing news outlets and the multitude of subsidiaries the companies have present a more complex challenge than is appropriate in this study considering the time and length limitation of the thesis. Therefore, these two questions were condensed to a single initial category for the initial data coding. During the course of the analysis the two sub-themes *everyday incidents* and *significant events* emerged under the main theme *cyber incidents*.

Overall, the categories created from the framework were topical categories. They were used to capture main characteristics of the disclosures. The categories were used as a part of the

qualitative content analysis in combination with categories emerging from the data to gain deeper insights into the risk disclosures and create further categories capturing nuances in the data.

## 3.5 Limitations

There are a few significant limitations to this study. First and foremost, the timeframe to perform the study was a period of about two months. This time period was non-negotiable since the study was set to be finished at a specific deadline. This limits the scope of the study to what may be properly finished in this time period. The second limitation of this study is the length of the work. Similar to the deadline, the limit on the number of words used in the study to a maximum of 25000 limits the scope of the study. Without these limits, the study could have been performed with a larger sample of companies or on the reports of more than solely three years.

Another significant limitation to take note of considering the type of analysis performed, qualitative content analysis, is subjectivity. While the process of data analysis has been formed systematically and in such a way as to decrease the warping of subjectivity, the effect of subjectivity can not be removed entirely in this type of analysis. What allows for a deeper understanding is both a strength and a weakness in the process.

Furthermore, language has been a limitation during the literature review of this research. The literature review was restricted to sources in English. In the case of legal sources, this limited the availability of national information and made it necessary to rely on official translations and supporting research instead of the actual laws.

## 3.6 Validity and Reliability

Validity and reliability are well established concepts and vital criteria to ensure quality in research (Bryman & Bell, 2011). Bryman and Bell discuss that while this is widely accepted in regards to quantitative research, there have been varying opinions on the subject when it comes to qualitative research. They mention that while some see no issue in utilizing the concepts in connection with qualitative research others see a need for adjusting their application or even replace them completely with other concepts they consider more appropriate.

In this study the concepts of reliability and validity are used to ensure quality in the work. Reviewing other options presented by Bryman and Bell revealed that suggested substitutes for the concepts still capture many of the same angles. Therefore, this study follows the recommendation of Mason (2002) who has chosen to simply adapt the concepts with a consideration for use in qualitative research.

Validity, as explained by Mason, refers to whether you are "'measuring' what you say you are" (2002, p. 39). To ensure that the data collection systematically identified risk disclosures in annual reports and that appropriate data was collected for analysis, this study followed the example set by other researchers in the field of risk disclosure and used keywords to search the reports and identify relevant passages of risk disclosures. To evaluate whether the passage should be included in the study it was compared to the previously mentioned definition of risk disclosure this study adheres to.

Reliability, as explained by Mason, refers to "the accuracy of your research methods and techniques" (2002, p. 39). Since the research design for this study includes qualitative content analysis a high degree of subjectivity marks the work. To minimize the degrading effect of subjectivity on the reliability of the study, the method followed has been highly structured, consensual coding (see Section 3.4.1) was utilized, and a high degree of transparency is ensured by the availability of the data analysed as well as the detailed description of the methodology of this study. Studying annual reports to analyse risk disclosures is a common practice in the field of risk disclosure as evidenced by the literature review.

Lastly, Mason (2002) also discusses the significance of generalizability. Bryman and Bell (2011) argue that this is part of external validity but since this study follows Mason's guidelines, generalizability is reviewed separately from validity. According to Mason, generalizability refers to "the extent to which you can make some form of wider claim on the basis of your research and analysis" (2002, p. 39). Since this study is exploratory, the focus is not on providing generalised conclusions regarding a wider population, rather the study seeks to increase understanding. Mason, however, discusses that qualitative studies often emphasize theoretical generalization over empirical generalization and so while the research does not generally seek to provide conclusions about a larger population the research may still provide implications for further generalization of the results. In this study, there is no reason to believe the conclusions drawn would not apply to other large international European-based publicly listed companies in the electric utility sector and as such the results provide an interesting foundation for further hypotheses in the topic to be tested in future research.

## 3.7 Research Ethics

Bryman and Bell (2011) note the importance of ethics in business research and describe four main ethical considerations - "whether or not harm comes to participants; informed consent; invasion of privacy; and deception" (p.122) - and four other concerns regarding management of data, copyright, trust and reciprocity, and affiliations and potential conflicts. Due to the nature of this thesis, ethical matters related to participants are not an issue, and the number of parties involved is limited. Furthermore, since the utilized data is publicly available, aspects such as data management or copyright do not bring additional challenges.

## 3.8 Chapter Summary

This chapter presents and motivates the methodology utilized to conduct the study. Firstly, an overview of the research approach and design is provided. The thesis consists of abductive exploratory research through qualitative content analysis, and it is longitudinal in nature. Secondly, the choice of sample companies and data collection is explained. To be able to select five large international European-based companies within the electric utility industry, a ranking of energy companies was utilized. The data was collected from their annual publications. The chapter further explains the process of the qualitative content analysis in detail and addresses concerns regarding limitations, reliability and validity, and ethics.

# 4 Analysis and Discussion

Following the qualitative content analysis process outlined in Section 3.4, several themes were identified in the sample companies' cyber risk reporting. The main themes are listed in Table 4.1, and these and all the sub-themes are also presented in Appendix D. In the following sections, the most interesting findings regarding the companies' cyber risk reporting practices are considered, and these main themes are guiding the structure of the discussion.

*Table 4.1 Main Themes in the Companies' Cyber Risk Reporting*

| **Theme** | **Meaning** |
|---|---|
| **Risk types** | Certain types of cyber risk |
| **Risk consequences** | Potential or realized consequences of cyber risk |
| **Risk mitigation** | Reduction/minimization of cyber risk or the impact of cyber risk |
| **Cyber incidents** | Cyber incidents that have occurred |
| **Information scope** | Information pertaining to the company or to companies in general |
| **Time orientation** | The focus is on the past or the future |
| **Time relevance of the risk** | Explanation of why the cyber risk has been or is relevant |
| **Vagueness** | Few details and short explanations |

## 4.1 Electricité de France (EDF)

An examination of EDF's cyber risk reporting unveils several interesting findings. There is an emphasis on *risk mitigation* with a focus on the future but details and specific targets for future development are lacking. Interestingly, the sub-theme *mitigation fallibility* is present and contributes to a more objective view of the company's handling of cyber risks. The company's reporting is relatively open with possible consequences, which clarifies the relevance of the risk to the reader but gives no information regarding incidents routinely faced by the company. While the reporting is clearly regularly updated, there are no large changes in EDF's cyber risk reporting from 2017 to 2019.

### 4.1.1 Risk Mitigation

An examination of EDF's cyber risk reporting reveals *risk mitigation* to be a strong theme. In fact, all three sub-themes *prevention*, *reduction of impact* and *mitigation fallibility* which are identified in Appendix D are present in the company's reporting. The exact information provided within this theme also changes between the years, indicating that the company regularly updates their risk mitigation information disclosures.

Clear examples of updated cyber risk mitigation disclosures are evident in both *prevention* and *reduction of impact*. The disclosures center around specific developments from the previous fiscal year and as such each year contains specific information. For instance, in 2017 EDF reworked some of their relevant policies, in 2018 EDF developed their crisis management system with a mind to cyber risks and in 2019 the company renewed the cyber risk insurance coverage.

While it is a criterion for quality according to Abraham and Shrives (2014), not all areas of risk mitigation are updated and there is a distant lack of details when their measures for dealing with cyber risks are mentioned. It is difficult for a reader to judge whether something has been done satisfactorily when it is described vaguely. The width of the risk reporting is more evident than the depth as many types of risk mitigation measures are mentioned without being discussed in detail.

The third theme, *mitigation fallibility*, refers to mentions of weaknesses in the company's cyber risk mitigation and it is interesting to note it in EDF's risk reporting. Berkman et al. (2018) note that shareholders do not respond well to negative terms in their risk reporting. This can work as an incentive against highlighting weaknesses in company risk mitigation and help explain why, while this theme is clearly present in EDF's 2017 risk reporting, see Table 4.2, it is only briefly there before it fades significantly in 2018 and is gone in 2019's risk disclosures. As evident in Table 4.2, in 2019, while the company admits that the risk of an attack is not eliminated, they do not explicitly address or mention that their risk mitigation measures may fail or be inadequate.

*Table 4.2 The Development of Mitigation Fallibility in EDF's Reporting 2017-2019*

| **Source** | **Quotation** |
|---|---|
| Reference document 2017 | "However, the Group cannot guarantee that these [back-up] programmes will not encounter technical difficulties during deployment or delays affecting their real-life implementation or that such programmes will make it possible to limit, in the event of a major disaster, the negative impact on the activity and the Group's financial position."<br><br>(EDF, 2018, p. 114) |
| Universal registration document 2019<br><br>*(corresponds to the reference document, the term utilized by EDF changes over the years)* | "However, the Group cannot rule out an attack on its information systems that would have consequences on the Group's operational activity, its finances, its legal position, in particular with regard to the integrity of personal data, or its reputation."<br><br>(EDF, 2020, p. 121) |

Proprietary cost theory, while explaining that managers want to avoid giving away proprietary information, also explains that they may be reluctant to give a skewed picture regarding the company's future for fear of legal repercussions and resulting costs. This demonstrates that influences pushing for an objective view of a company's risk mitigation are present. These may have played a role in EDF explicitly pointing out that their risk mitigation efforts are not foolproof.

### 4.1.2 Future Orientation

While EDF's cyber risk reporting is clearly marked by *past orientation* through the mentions of past developments and progress, a clear *future orientation* is also present. EDF's reporting lacks specific targets regarding the development of their cybersecurity but cybersecurity is connected to their overall strategic future development. This is made very clear as cybersecurity is mentioned as one of five areas around which their R&D efforts revolve when it comes to information technology. While specifics and short-term goals are lacking, it is emphasized to readers that cyber security is a key area considered in the development of the company.

According to institutional theory, companies may emulate others to live up to general standards when it comes to their reporting. The literature review of this thesis demonstrates the growing focus on cyber risk in the business world and especially the energy sector. The lack of detail

regarding future goals in the area of cyber risk makes it difficult to determine whether this part of EDF's risk disclosure could be a response to the overall emphasis on the significance of cyber risk.

### 4.1.3 Cyber Incidents

Abraham and Shrives (2014) emphasize the importance of the description of risk experiences as that provides some proof that the disclosures are not mere boilerplate (see Section 2.4). However, consistent with some previous findings about the lack of discussion about actual cyber incidents in companies' reporting (Section 2.2.1) and institutional and proprietary cost theory, EDF does not mention any cyber risk experience in 2017, 2018 or 2019. Yet, it is acknowledged that there are such experiences, since, for example, the unit responsible for reporting on information systems security incidents is mentioned in 2019. Little information is provided, leaving stakeholders ill-informed.

## 4.2 Iberdrola

A review of Iberdrola's cyber risk reporting in 2017, 2018 and 2019 reveals some interesting developments. A shift in the information provided to include more *company-specific information* is noted in both the theme *risk consequences* and the theme *risk mitigation*. An inclusion of specific numbers regarding data breaches in 2018 and 2019 which was not provided in 2017 shows some development in the theme *cyber incidents* as well. While a lack of details prevails through the three years, there are distinct signs of changing habits in Iberdrola's cyber risk reporting practices. The theme *company-specific information* is increasing in strength.

### 4.2.1 Risk Types

Iberdrola's reporting of different types of cyber risk stands out. The same sentence listing a wide range of cyber risks is set forth each year, remarking aspects such as unauthorized access, interruption and degradation of information systems, among other risk types. While this remains unaltered from year to year, in 2019 cybersecurity risk is further elaborated with the passage in Table 4.3.

*Table 4.3 Addition to Iberdrola's Risk Reporting on Risk Types in 2019*

| **Source** | **Quotation** |
|---|---|
| Annual financial report 2019 | "The main risks are:<br>- Risks related to Operations Technology (OT), such as IT and communications systems used to manage industrial operations (production, management and distribution of energy) or physical safety systems (fire protection, CCTV, alarm reception centres).<br>- Risks related to admin or customer interfaces (TI), in particular violation of information in hem [sic], under the umbrella of General Data Protection Rules (GDPR) in Europe and other countries.<br>- Other cybersecurity risks having an impact on reputation."<br>(Iberdrola, 2020a, p. 263) |

The information about which type of cyber risks Iberdrola is exposed to is more detailed than previously. As evidenced by the quote above, general terms like "operations technology" are clarified with examples of what this refers to in the case of Iberdrola. This shift in favour of higher transparency is provided without adding a lot of words or contextual information, perhaps this would be shown approval by Abraham and Shrives (2014) since the reporting is becoming more detailed without adding a lot of unnecessary text for the reader to sift through.

### 4.2.2 Risk Consequences

The four sub-themes of *risk consequences* - *magnitude of impact*, *specified type*, *company focus* and *stakeholder focus* all emerge from Iberdrola's reporting. There are imprecise remarks about economic, operational and reputational consequences, and the magnitude of impact is described as potentially huge, concerning the whole country's energy supply. Related to this, it is mentioned in 2019 reporting that a cyber attack could harm even other suppliers in addition to Iberdrola, which falls into stakeholder focus. Additionally, each year it is explicitly noted that the realization of cyber risk would have consequences for customers.

The presence of this variety of sub-themes emphasises that the company presents a quite well-rounded view of potential consequences of cyber risks. This theme further also sees a development over the three years included in this study. The theme is notably weaker in 2017 and 2018 with few details and yet in 2019 there is a clear development in the context provided

for possible consequences. The company gives more exact information about how cyber assets are tied into their infrastructure before referencing possible consequences.

This further entails a change in the theme *information scope* in the company cyber risk reporting. In 2019 the sub-theme *company-specific information* regarding risk consequences is stronger which is in line with good practice according to Abraham & Shrives (2014). While this shift is not necessarily indicative of a lasting change in the reporting towards a higher degree of transparency, it does raise the question of whether this could be the case.

### 4.2.3 Risk Mitigation

All three sub-themes of *risk mitigation* - *prevention*, *reduction of impact* and *mitigation fallibility* - can be found in Iberdrola's cyber risk disclosures. For example, there are remarks about insurance, collaborations and education, and an emphasis is placed on describing the officers, committees and divisions responsible for different cyber risk related activities. It varies whether the information is updated during the years and whether it is company-specific or general. Nevertheless, the most intriguing aspects concern education and fallibility.

Already in 2017 it is noted that employees are offered cybersecurity training. Interestingly, this rather vague information exists in each year's reporting, but the disclosure also changes over the years to include more details. In both 2018 and 2019 Iberdrola both updates and extends the information with more exact examples of how they work with education to mitigate cyber risk. In 2018 a new on-boarding programme is mentioned and it is said to include information about cybersecurity. In 2019 the programme is still recognized but, in addition, there is a remark about virtual training courses with names included providing further information about them. One example is "Cybersecurity risk evaluation in purchases" (Iberdrola, 2020b, p. 159). This illustrates that the disclosure becomes more company-specific over time and is regularly updated, which are signs of good quality reporting (Abraham & Shrives, 2014).

*Mitigation fallibility* is present in Iberdrola's reporting in 2018. There is a comment about the fact that operational (including cyber) risk cannot be perfectly eliminated by acquiring insurance. It is a general statement but it nonetheless indicates vulnerability and explicitly mentions that insurance does not cover all eventualities.

### 4.2.4 Cyber Incidents

Iberdrola's cyber risk reporting is the only one of the companies in this study who discloses not only on smaller cyber incidents but also includes a mention in 2017 of a larger scale cyber attack the company was affected by during the year. In other words, their risk reporting held both sub-themes of the main theme *cyber incidents*: *everyday incidents* and *significant events*. The presence of this second sub-theme does not, however, weigh very heavily in the cyber risk disclosures.

The mention of the attack is brief, see Table 4.4, and seems to indicate this was a well-known phenomenon. An article by Wong and Solon outlines a large-scale international ransomware

cyber attack on that date and describes the event as having been targeted at "nearly 100 countries around the world" (2017, n.p.). The massive size of the scale and scope of the event indicates that this was likely a well-known event and an issue therefore pertinent for the company to address in their reporting. The details though, are sparse and what is emphasized by the company is that the impact of the attack did not cause any material consequences. The tone is positive.

*Table 4.4 Iberdrola's Mention of the Cyberattack 2017*

| **Source** | **Quotation** |
|---|---|
| Annual financial report 2017 | "The international ransomware cyberattack that occurred on 12 May 2017, which only partially affected some of the Iberdrola group's activities in Spain. The cybersecurity measures implemented at all businesses and corporate functions and the current action protocols ensured that no critical service, operation or customers were at any time significantly affected."<br><br>(Iberdrola, 2018, p. 369) |

The other two years show no mention of significant events, and whether this depends on the fact that no such events have taken place in 2018 and 2019 or they have and the company chose not to report on them is unclear. Institutional theory emphasises the influence of institutional forces on how companies shape their risk reporting and with highly publicized events of a massive size there would likely be a lot of pressures for the company to address the 2017 attack in their reporting. With only three years examined it is difficult to know whether the company only chose to report on the event due to it being publicized or because they generally report on this type of events in their reports even when they have gathered less or little attention.

The second sub-theme, *everyday incidents*, is present in the reports from 2018 and 2019 where the company reports on data breaches in relation to customer data. Specific numbers are presented for both years, giving a closer level of detail than the reporting on the cyber attack in 2017. The numbers are also set side by side with the numbers from the previous year, highlighting the change and making it easy for the reader to compare and spot any developments. This further makes it clear that the risk reporting is regularly updated, which is in line with Abraham and Shrives' (2014) criteria for quality risk reporting, as is discussing specific incidents even if the level of detail is not very high.

It is worth reflecting whether the 2017 cyberattack has contributed to the overall developments noted in Iberdrola's cyber risk reporting. The company has become more detailed and company-

specific with their disclosures. This provides stakeholders with a more accurate idea of how Iberdrola specifically handles cyber risk rather than energy companies in general.

## 4.3 Enel

The main theme most emphasised in Enel's risk reporting is *risk mitigation*. Less attention is paid to *risk consequences* and *risk types*, and while no *significant events* are discussed, the company does report on *everyday incidents*. The reporting is updated every year and it focuses on company-specific rather than general information, which is in line with good risk disclosure practice according to Abraham and Shrives (2014). Furthermore, there is also an increase in transparency and detail regarding both *risk consequences* and *cyber incidents* from 2017 to 2019.

### 4.3.1 Risk Mitigation

The most prominent theme identified in Enel's cyber risk reporting is *risk mitigation*. As demonstrated in Appendix D, the theme contains three sub-themes, two of which are present in Enel's reporting, *prevention* and *reduction of impact*. The first sub-theme is clearly dominant and a large part of the risk reporting outlines how the company works with preventing cyber risk from adversely affecting the company.

The exact information within this theme changes during these three years. Comparing the risk disclosures of 2017, 2018 and 2019 it is worth noting that new information in this theme emerges every year. New initiatives and efforts are mentioned all three years. In other words, the information is updated yearly at least partly despite the recurrence of certain descriptions and phrasings. A prominent example of Enel's work with preventing cyber risk is their education initiatives.

Education initiatives as a means of risk mitigation is clear in all three years of Enel's cyber risk reporting. The company presents both specific education modules for certain employees working closer with technology and work on a broader scale towards forming a culture facilitating secure use of cyber assets. Cyber risks are therefore presented as risks not just concerning specific groups or business functions within the company, but as risks relevant to the entire company. This broad view of the risks is further widened in 2019 when the company goes on and mentions working towards being able to educate not just company employees but also certain external parties.

Another interesting example in Enel's cyber risk reporting is the steady pursuit of specific goals which can be observed throughout the three years. In addition to mentioning past initiatives and having a *past orientation*, Enel's cyber risk disclosures have a strong *future orientation*. The company presents specific targets for increasing their cyber security, for example setting a target security coverage rate for their web applications, and these numbers are updated every year allowing the reader to follow the company's progress. They provide quantified, company

specific and updated information - the first is generally lacking in risk reporting (Mazumder & Hossain, 2018) and the latter two are signs of higher quality risk disclosure (Abraham & Shrives, 2014).

While the other sub-theme, *reduction of impact*, is less prominent, it is also present in the reporting. In 2019, for example, the company reveals that they have insurance toward IT risks. They also reference specific policies in the event of breaches, which outline which actions should be taken to minimize the impact.

### 4.3.2 Risk Consequences

This theme in Enel's cyber risk reporting is interesting due to the development that occurs from 2017 to 2019. A steady increase in specifics from year to year is noted. The view of possible consequences of cyber risk presented to shareholders broadens.

The sub-themes of risk consequence evident in the company's disclosures are: *specified type*, *stakeholder focus*, *company focus* and *magnitude of impact*. In 2017 all but *stakeholder focus* are present, although weakly. In 2018 *specified type* strengthens as new kinds of consequences are mentioned and *stakeholder focus* emerges, meaning that the company relates possible risk consequences not just to the company themselves but to external stakeholders. Table 4.5 exemplifies the change. In 2019, this development continues through various types of consequences, and all the four sub-themes are present. Nonetheless, during all three years there are no details, the magnitude is expressed broadly, and the information remains general.

*Table 4.5 Change in Specified Type from 2017 to 2018 and the Emergence of Stakeholder Focus in 2018 in Enel's reporting*

| **Source** | **Quotation** |
|---|---|
| Consolidated non-financial statement 2017 | "highlighting a possible risk, in extreme cases, of companies' and organizations' normal operations grinding to a halt"<br><br>(Enel, 2018, p. 16) |
| Sustainability report 2018 | "a large-scale blackout could have an impact on individuals, businesses, institutions and essential services"<br><br>(Enel, 2019, p. 126)<br><br>"could affect business continuity, ownership, reputation and profitability of the Enel Group" |

| | |
|---|---|
| | (Enel, 2019, p. 127) |

While the overall lack of detail regarding potential consequences is understandable since companies generally do not want to present themselves as vulnerable, it could also be worth asking what very detailed risk consequence descriptions would accomplish in terms of informing the reader. After all, the potential consequences mentioned by Enel illustrate the relevance of cyber risk, which is a sign of good-quality disclosure (Abraham & Shrives, 2014). However, is it enough to impart the materiality of the risk or should more detailed accounts be provided?

The development noted in the disclosures is interesting since there is an increased transparency and increased degree of detail provided in the disclosures regarding cyber risk consequences. Institutional theory emphasises the influence of outside pressures on companies. This raises the questions of whether the overall trend towards more varied and transparent corporate reporting has contributed to the changes evident in Enel's cyber risk disclosures.

### 4.3.3 Cyber Incidents

In all three years, the sub-theme *everyday incidents* is present in Enel's cyber risk reporting. The number of different types of incidents, such as viruses and spam emails, is mentioned. This practice fits with what Abraham and Shrives (2014) expect from risk reporting - Enel's description of the incidents is company-specific, updated regularly, implicitly explains the relevance of cyber risk, and discusses actual risk experiences.

The theme strengthens significantly after 2017. In 2017, only the number of identified and blocked incidents daily and during the year is given. Improvement occurs for 2018 and 2019 since there is more detailed information; for example, the team responsible for handling incidents and the system to classify the incidents according to impact are mentioned. Yet, although it is mentioned that there had been one level 3 incident in 2018 (the highest level is 4) and ten such incidents in 2019, all that is noted is that there was no significant damage. Table 4.6 provides an example of this.

*Table 4.6 Example of Enel's Cyber Incident Disclosure in 2018*

| **Source** | **Quotation** |
|---|---|
| Sustainability report 2018 | "Those classified at level 2/3/4 have a potential impact on the Group and are managed by involving the interested parties. During 2018, CERT responded to 39 computer security incidents with impact level "2" and 1 incident with impact level |

| | |
|---|---|
| | "3". In all the detected cases, all the procedures were activated and no damage was caused to the company assets."<br><br>(Enel, 2019, p. 127) |

Overall, attention is given to the positive aspects. The reporting reveals that there are numerous incidents each day, but it is emphasized that the systems and procedures allow Enel to block them and protect its operations. This is not surprising considering proprietary cost theory and institutional theory as well as potential stock market effects as discussed previously.

## 4.4 SSE

SSE's cyber risk reporting has no clearly dominant theme but keeps all information rather brief and generally with little to no specifics. While the cyber risk disclosures are not identical between the years, there is very little noted development and changes in the company's annual publications in the three-year period. However, there are indications of regular reassessments regarding the state of cyber risk at SSE. For example, the cyber risk section includes 'developments', indicating the relevance of the risk (connected to the framework by Abraham & Shrives, 2014), and in each year's report something current is mentioned in addition to emphasizing the growing risk of severe cyber attacks. Networks and Information Systems (NIS) Directive and General Data Protection Regulation (GDPR) are noted in 2017/2018, GDPR and Brexit in 2018/2019, and the coronavirus and the sale of SSE Energy Services in 2019/2020. This is very illustrative of SSE's cyber risk reporting in general - there are some signs of updates through short remarks about current matters, but little company-specific information is presented.

### 4.4.1 Risk Mitigation and Cyber Incidents

While *risk mitigation* is not a dominant theme in SSE's cyber risk reporting, it is still very much present. The sub-themes *prevention* and *reduction of impact* are noted. The former is the most prominent of the two but both get little attention and see little development over the three years.

The mitigations listed in the cyber risk reporting is reused word-for-word throughout all three years and contains no examples or numbers which change. In other words, this section of the reporting has not seen regular change in the period reviewed. The company's cyber risk reporting does not live up to the criteria set out by Abraham and Shrives (2014) of regularly updated risk disclosures. It is however in line with following a set habit which institutional theory explains that companies easily do and that they may be reluctant to change. It further makes it easy for company management to keep up their existing standard of transparency, which Graham (2005) noted as a worry for executives. This part of their cyber risk disclosures

seems to be formed more for the convenience of the management and less in the interest of the investor.

The new information provided in the theme is sparse but includes examples of specific cyber risk mitigation initiatives like the launch of a new education module in 2019/2020. This indicates that while there is a lack of updates in the overall risk mitigation information, the section is regularly reviewed and the company is prone to adding a bit more details at times. It does, however, make it difficult for the reader of the disclosures to judge how the company is handling their exposure to cyber risk and raises the question whether their purpose is to provide useful information or keep up a facade of transparency without actually providing much specific information which could leave them vulnerable.

Another criterion set out by Abraham and Shrives (2014) for quality risk disclosures which is arguably left unmet is the one that companies should disclose information about previous risk events or incidents. SSE's cyber risk reporting is lacking mentions of previous cyber incidents except for a short mention which informs the reader that real life examples of events are used in their scenario analysis. These are not necessarily events previously experienced by the SSE, however, and no detailed information about the events are given. The reader is not provided with any further information about previous cyber incidents which has affected the company and so the theme of *cyber incidents* is very weak in the company's cyber risk reporting.

### 4.4.2 Risk Consequences

While consequences are not described explicitly, the potential impact of cyber risk is illustrated on a figure relative to the other principal risks in 2017/2018 and 2018/2019. This demonstrates the presence of the sub-theme *magnitude of impact*. The notable potential impact illustrates the relevance of the risk, albeit in a limited way. In 2019/2020 the corresponding figure is somewhat different due to the coronavirus and does not illustrate the impact in the same way. Furthermore, in all three years the risk is considered to have increased in materiality but the information is conveyed in the same manner, making it difficult to know whether the information has actually been updated.

## 4.5 EnBW Energie Baden-Württemberg (EnBW)

EnBW's cyber risk reporting really stands out compared to the other companies in this study. A review of the company's annual publications reveals significantly sparse cyber risk reporting. While cyber risks are mentioned among the risk factors each year, it is not considered material enough for the company to elaborate on anything concerning the risk. Table 4.7 and Figure 4.1 show what EnBW discloses on cyber risk.

*Table 4.7 EnBW's Cyber Risk Reporting in Whole*

| **Source** | **Quotations** |
|---|---|
| Integrated annual report 2017 | *In the opportunity and risk map, within the operative category, subsection infrastructure:*<br><br>• "Plants/Grids/Storage/IT"<br>• "Information security/confidentiality"<br>• "Crime/sabotage/terrorism"<br><br>(EnBW, 2018, p. 91) |
| Integrated annual report 2018 (extended version) | *In the opportunity and risk map, within the operative category, subsection infrastructure:*<br><br>• "Plants/grids/storage/IT"<br>• "Information security/confidentiality"<br>• "Crime/sabotage/terrorism"<br><br>(EnBW, 2019, p. 116) |
| | *In the corporate governance section, under compliance:*<br><br>"EnBW holds a compliance day every year. The event was held on 22 October 2018 in Karlsruhe and provided the around 115 participants with a varied programme that covered themes such as data compliance and the risks posed by cyber attacks and how to avoid them."<br><br>(EnBW, 2019, p. 58) |
| Integrated annual report 2019 (extended version) | *In the opportunity and risk map, within the operative category, subsection infrastructure:*<br><br>• "Plants/grids/storage/IT<br>• "Information security/confidentiality"<br>• "Crime/sabotage/terrorism"<br><br>(EnBW, 2020, p. 100) |

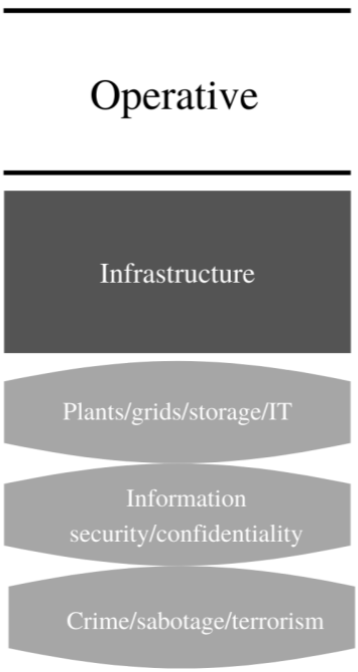


*Figure 4.1 An Illustration of a Zoomed-in Section of the Opportunities and Risk Map in EnBW's Integrated Annual Reports*

EnBW's cyber risk reporting includes the themes *risk types* and *risk mitigation*, and while neither of the themes is prominent, the latter is even less so. The company provides very little information regarding risk mitigation in 2018 and nothing at all in 2017 or 2019. The recognition of cyber risk, however, means that there are likely significant efforts at mitigating the risk but the specifics of this are not communicated in their annual publications. This makes it difficult for readers to evaluate the company's handling of cyber risk.

Considering the points raised in proprietary cost theory, that companies have incentives to shape disclosures to their advantage and leave out certain information completely to protect themselves, it raises the question of whether this is true or not. The literature review in this study clearly emphasises the significance of cyber risk in the electric utility sector and the 2015 and 2016 attacks on Ukrainian companies certainly demonstrate possible consequences of cyber attacks for companies in this sector. It is possible EnBW has other motives than lack of materiality for keeping their cyber risk disclosures short.

## 4.6 Overview: Differences and Similarities

This section provides an overview of the reporting practices of the companies as a group. This thesis has revealed several interesting similarities between the cyber risk reporting of the companies included in the study as well as some intriguing differences. A discussion on these now follows.

### 4.6.1 Information Scope

The theme of *information scope* holds two main themes, *general information* and *company-specific information*, the latter of which is considered better practice (Abraham & Shrives, 2014). There is no clear consistency in the sample companies when it comes to this. Their disclosures generally contain both types of information but *general information* is more prominent.

It is further interesting to note where this theme intersects with other themes. *Company-specific information* is more common in connection with *risk mitigation* while *general information* is definitely dominant when it comes to *risk types* and *risk consequences*. In other words, companies seem to be more willing to reveal information when it does not leave them vulnerable. However, it is debatable to what extent risk types and consequences can be truly company-specific.

### 4.6.2 Risk Types and Risk Consequences

The theme *risk types* is present in all sample companies' risk disclosures. In addition to the widely utilized term cyber attack, other examples include hacking, data breaches, and viruses. The theme does not have a strong presence and the information in this theme is generally presented shortly and with no details. It is easy to leave the risk description vague. The one company that stands out is Iberdrola since more precise examples are given.

*Risk consequence* is a theme which is present in all but one of the companies' cyber risk disclosures. The information is generally short and unspecific and yet four sub-themes emerge from the data: *magnitude of impact*, *specified type*, *company focus* and *stakeholder focus*. The first two are the most prominent sub-themes but their presence varies between companies. EDF, Enel and Iberdrola mention different types of consequences, and examples include reputational damage, data breaches and operational obstacles. This is in line with previous research by Gao, Calderon and Tang (2020), Héroux and Fortin (2020) and Li, No and Wang (2018) who note that these are common points of concern for companies in connection with cyber risk. As for magnitude, EDF, Enel and Iberdrola utilize vague terms. SSE's reporting is different from this since the focus is on the magnitude of cyber risk relative to other risks. Lastly, EnBW does not discuss any consequences directly related to cyber risk.

As can be seen, most companies examined mention something about the magnitude of impact. However, the terms utilized are rather general, which is on the other hand understandable given the difficulties in estimating the costs of the realization of cyber risks as noted in Section 1.1.2. There is no quantification, and that conforms to earlier research (Mazumder & Hossain, 2018).

The weak focus on this theme in the cyber risk disclosures analysed can be explained by previous research. Negative terms can have a negative effect on company stock price (Berkman et al., 2018). The information provided in these disclosures emphasises the relevance of the risk while providing little more. Proprietary cost theory explains that companies may present information in a way which avoids revealing much and leaving them vulnerable. They battle

the need to present a fair view of the company to the stakeholders and the need to protect their operations from malicious third parties.

While the information presented in regards to this theme is limited, it would be worth asking whether much more would be of use to the stakeholders. Abraham and Shrives (2014) mention that a lot of text may actually be a bad thing unless the content is utilized well. Would the time perspective, for example, be of value to investors and other stakeholders? More insight into whether long-term or short-term consequences are more likely, for example, could be of interest. Either way, the focus in the company reporting naturally shifts away from the negative potential consequences as the publications, while useful documents for stakeholders, have been produced by company management whose interest in presenting a strong and positive view of the company is clear.

### 4.6.3 Risk Mitigation

*Risk mitigation* is present in all companies' reporting. This theme is often notably strong, has a relatively high level of detail and tends to contain examples of company actions and initiatives with the purpose of risk mitigation. The prominence of this theme in the companies' reporting is not surprising considering it allows the companies to highlight their strengths and what they have done well to protect their operations and therefore the interests of the stakeholders, the readers of the reports. It has also been found that cyber risk management reporting can reduce the contagion effect, i.e., the negative effect on the stock price of a company when a similar company has suffered a cyber attack (Kelton & Pennington, 2020; Section 2.2.3).

The weakest sub-theme of risk mitigation is *mitigation fallibility*. While it has been noted in two of the companies, it is significantly weaker in its presence than *prevention* and *reduction of impact*. This theme emphasises the potential weaknesses or fallibility of the mitigation measures and as such provides a more objective and less positive tone regarding the state of the company's risk position and the likelihood of a cyber incident impacting the company. That shareholders do not appreciate negativity in the company cyber risk reporting has been suggested (Berkman et al., 2018) and may explain the weakness of this sub-theme.

A common example within *risk mitigation* mentioned in the companies' reporting are cybersecurity policies and committees. It is less common for the companies to reference specific initiatives taken to promote the security, although Enel stands out with their reporting here as the company provides specific targets for the future and mentions several recent initiatives by the company. The overall focus on policies is interesting and may possibly be explained by proprietary cost theory. Mentioning policies or committees emphasises a company's work with cyber risk management without actually revealing much of anything. The company is then not risking revealing information which may leave them vulnerable to malicious attention from third parties, which proprietary cost theory suggests is a common worry. It gives the impression of transparency.

### 4.6.4 Incidents

The discussion of actual risk experiences can be regarded as good practice (Abraham & Shrives, 2014), but the findings in this study vary. EDF, EnBW and SSE are silent about them, Iberdrola mentions the data breaches and the 2017 ransomware attack, and Enel presents the number of incidents and some related information. While the information is company-specific, it is not detailed. Interestingly, the notable international ransomware attack in 2017 was only discussed by Iberdrola. However, the news give the impression that it hit Spanish companies harder (Wang & Solon, 2017), which could be one explanation for why the attack is not considered by other companies.

In general, the findings are not surprising in light of previous research about the reporting on cyber incidents (Section 2.2.1) and the potential negative stock market effects (Section 2.2.3). This is in line with proprietary cost theory, indicating that the electric utility companies examined might not desire to share all internally available information. Also, when incidents are mentioned, the focus is on successful mitigation rather than the actual details of the incidents. Furthermore, institutional theory can explain why vagueness is common for all the companies, since companies can avoid some uncertainties by following the general practice within the industry.

### 4.6.5 Vagueness

An interesting aspect emerging in the companies' reporting as a whole is the recurring notice of a lack of details, explanations or descriptions. When more information is present, it is usually kept short. This aspect of cyber risk reporting is captured by the theme *vagueness*, examples of which are provided in Table 4.8. Keeping the information reported sparse in detail makes it difficult for an investor to examine the company's handling of a risk and determine for themselves whether the company's actions are appropriate.

*Table 4.8 Examples of the Theme Vagueness*

| **Company and source** | **Quotation** |
|---|---|
| SSE<br><br>Annual report 2017/2018 | "Key technology and infrastructure risks are incorporated into the design of systems and are regularly appraised with risk mitigation plans recommended."<br><br>(SSE, 2018, p. 29) |
| Enel<br><br>Sustainability report 2017 | "Finally, the activities to improve the protection of the Enel Group's websites continued, using advanced technologies to make visitor information secure, to protect |

| | |
|---|---|
| | sites from hacking of applications, to make sites faster and to mitigate attacks."<br><br>(Enel, 2018, p. 158) |

It is also worth noting, however, that in the case of cyber risk it may not be a bad thing to restrict the amount of technical info regarding their mitigation measures. Would the average reader understand if companies elaborated more or would it just constitute extra text to sift through? Restricting the details may further be of interest to stakeholders as well as management, if malicious third parties decide to take advantage of a company being transparent both the company and the investors stand to lose.

### 4.6.6 Change

As the discussion has shown, there are highly varying findings regarding updates in reporting practices. Sometimes parts of disclosures remain completely unchanged, sometimes the wording is different but the content the same, and sometimes updates are made and new aspects added. There are notable differences not only between companies but also within companies in terms of specific parts of the cyber risk disclosure. According to institutional theory, unaltered reporting can be a way to avoid uncertainty, but regularly updated information is a sign of good quality (Abraham & Shrives, 2014).

In contrast with updated information, more fundamental overall changes in how the company reports on certain types of information were also noted in this study. The most significant over-the-years developments are the fading of EDF's *mitigation fallibility*, the increasing preciseness and substance in Iberdrola's reporting, and the varying changes in Enel's disclosures. While more precise information may be appreciated by stakeholders, it can also make the company vulnerable as indicated by proprietary cost theory. Reluctance to change can be explained by institutional theory since institutional pressures and uncertainty avoidance can be the reason for routine reporting. Small or no changes are likely quite convenient for the company management.

Considering the increasing cyber risk in the business climate, especially in the energy sector, it is interesting that no large developments have been noted from 2017 to 2019 in this study across the five examined companies. Perhaps the time scope is too small for any changes to be revealed, or perhaps the materiality of the risk has been evident to the companies for years already and as such not much has changed in how they relate to cyber risks. To really capture the development of cyber risk disclosures in the electric utility sector, a study over a larger amount of years would be necessary.

### 4.6.7 The Case of EnBW

It is interesting to see that despite the more elaborate cyber risk reporting of the other four examined companies, EnBW has kept their cyber risk disclosure short. This goes counter to institutional theory according to which companies tend to report similarly to their peers in an effort to prove the quality of their reporting lives up to general standards. Are these pressures not a factor in EnBW's decision, or are there different peers or influences having a stronger effect on their actions? As Section 4.5 mentions, this raises the question of whether the company deliberately has kept their disclosures brief to avoid having to leave themselves vulnerable and open to scrutiny. This would be in line with proprietary cost theory.

### 4.6.8 Theoretical Connections

The two theories chosen for the thesis, proprietary cost theory and institutional theory, seem to explain several aspects of the findings regarding cyber risk reporting in this study. There are, however, also a few intriguing instances where the data does not follow the theories presented. This section provides a short overview of the connections made between the data and the theories in the analysis of this study.

Consistent with proprietary cost theory, there are a few ways through which the companies examined avoid disclosing sensitive information that might leave them vulnerable. *Vagueness* is evident in each company's cyber risk reporting, and there appears to also be a strong focus on the positives; for example, the companies generally emphasize their risk mitigation strategies and procedures. Moreover, the companies do not discuss actual cyber incidents or if they do, the successful risk management is highlighted instead of the characteristics and consequences of the incidents. In other words, the companies are significantly more forthcoming when it comes to information which either may improve their image, or simply not harm their image.

Institutional theory argues that company reporting habits converge as they mimic their peers to uphold the industry standard. In this thesis four out of five of the companies studied pay significant attention to cyber risk and, as outlined above, have a positive tone and an emphasis on *risk mitigation* in common. The fifth company, EnBW, also acknowledges cyber risk but their reporting is significantly sparse in comparison to the other companies'. This is counter to institutional theory as EnBW's cyber risk reporting differs from that of their peers. One possible explanation could be that the influences implied by proprietary cost theory are stronger than those indicated by institutional theory.

Furthermore, there are also varied findings noted regarding cyber incident reporting, both in whether it is present and how it is present. This small sample makes it difficult to say for sure, but it is possible that a clear industry standard regarding this issue has not emerged due to the sensitive nature of the information and the varying incentives for transparency and privacy. This is a part of cyber risk reporting where proprietary cost theory is more satisfying in explaining what the data is revealing.

Finally, this study has revealed few and gradual changes in the cyber risk reporting over the three-year period. Institutional theory explains that companies are slow and resistant to

changing their reporting habits as it is convenient for management to avoid uncertainty. Proprietary cost theory highlights the sensitivity of the matter and as such explains possible obstacles for increasing transparency. Despite this, the change in Iberdrola's reporting was evident as the disclosures increased in detail over the three years. The slow pace is easily explained by the theories but the increase in transparency is less evident. Perhaps the overall societal focus on cyber risk and the changing nature in risk reporting to include more non-financial information are significant institutional pressures here and have influenced Iberdrola to change their reporting.

## 4.7 Further Discussion

Considering the nature of corporate reporting, companies report on themselves in circumstances where they have incentives to present themselves in a good light. An interesting question is whether the companies' cyber risk reporting appears to be for show or genuinely reflects the attention paid to the risk internally. This further raises questions regarding the morality of cyber risk disclosures. As Section 2.3 emphasises, cyber risk is not explicitly required by law in the EU and it is up to individual companies whether it should be included in their risk disclosures. Further, it is questionable what difference mandatory cyber risk reporting would make. Following the law does not imply that companies do not present their disclosures in a way that makes them be seen positively.

The companies in this study all mention cyber risk in their annual publications. The disclosures consist of a mix of company-specific and general information. Institutional theory explains that the overall societal emphasis on cyber security could be working to pressure companies to disclose on the subject. Is their reporting, then, actually reflective of the internal attitude and handling of the risk or simply an attempt to pacify external stakeholders?

According to Abraham and Shrives (2014), risk disclosures containing company-specific information tend to be more substantive while disclosures containing general information tend to be symbolic. While a mix of both is evident in the data analyzed in this study there are definitely signs of some companies leaning more in a certain direction. Enel, for example, has cyber risk disclosures which includes specific targets and initiatives they have or are pursuing in order to mitigate cyber risk. EnBW, on the other hand, has very sparse disclosures of mainly general information. General information on the risk may give the impression of the company handling the risk without providing specific examples which may be checked for accuracy.

A certain degree of vagueness, however, is to be expected and is probably unlikely to disappear since the risk of leaving the company vulnerable will keep management from giving away too much. This can also work in the favor of stakeholders if it protects the company and facilitates good performance. This is the case especially in the electric utility sector since it is critical for the functioning of the whole society. The arguments for and against transparency leaves the authors of this study with the question of what the ideal balance of transparency regarding cyber risk actually is.

## 4.8 Chapter Summary

This chapter presents the analysis of the data collected for this study. The companies are first examined individually and the themes and developments in their individual cyber risk reporting are presented. The companies are then examined as a group in a cross-case analysis and significant differences, similarities and developments in their cyber risk reporting are discussed. The discussion is connected to the literature review and the theoretical information in Section 2. The main findings involve the strong presence of *risk mitigation*, *vagueness* and positive tone. Moreover, change over the years is highly varying depending on the company, and EnBW's cyber risk reporting differs from the other companies.

# 5 Conclusion

## 5.1 Research Aims and Objectives

As outlined in Section 1.2, the aim of this study has been to investigate the cyber risk reporting practices of the five large publicly listed international European-based electric utility companies chosen for this study and how the disclosures have changed over the last few years. The selected companies were Electricité de France (EDF), Iberdrola, Enel, SSE and EnBW Energie Baden-Württemberg (EnBW). Accordingly, two research questions were formulated: "What and how do large international publicly listed European-based electric utility companies report on cyber risk in 2017, 2018 and 2019?" and "How has the companies' cyber risk reporting changed during these three years?". To answer these questions an exploratory research approach was chosen and the study conducted for this thesis consisted of a qualitative content analysis of cyber risk disclosures collected from the sample companies' annual publications.

Furthermore, three main objectives were formulated to ensure the questions were properly investigated. The first objective was to analyze the cyber risk disclosures from 2017, 2018 and 2019. The second objective was to analyze the development of the companies' cyber risk reporting practices by examining the change in the cyber risk reporting practices over time. The third and final objective was to perform a cross-case analysis and examine the cyber risk reporting practices of the sample companies as a group and highlight similarities and differences. The main findings of the analysis presented in Section 4.6 can be summarized in five points as demonstrated by Figure 5.1.

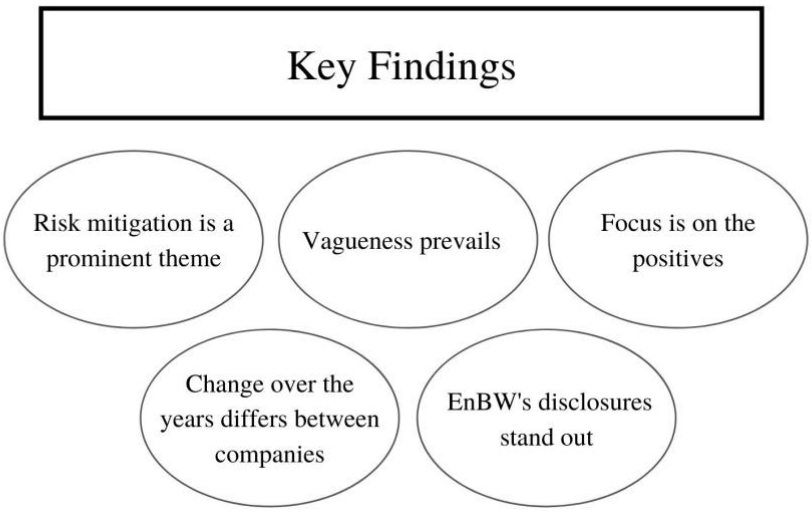


*Figure 5.1 Summary of Key Findings*

The prominence of the theme of *risk mitigation* was noted due to the presence of the theme across all companies included in this study, as well as the relatively high degree of company-specific information provided in connection with the theme. This theme is marked by a higher degree of detail than other emergent themes such as *risk consequences* and *risk types*. The prominence of the theme is not surprising considering the nature of annual publications, companies reporting on themselves, which naturally leads to a certain bias and a wish to represent the company well. Providing information on risk management can further also work to reassure investors when other similar companies have been the victim of cyber incidents (Kelton & Pennington, 2020).

The second main finding involves the theme *vagueness*. The information provided by the sample companies in their cyber risk disclosures is generally lacking details, and in some cases the information is not company-specific at all but consists of statements which could apply to any company in general or any company in their industry. This practice is in line with proprietary cost theory which explains that there may be a significant difference in the internally available information on a risk and the information which is disclosed externally. The theory attributes this to management worrying about revealing information which would make the company more vulnerable and so they have incentives to create risk disclosures with less or more imprecise information in order to protect the company's interests.

The third main finding follows naturally after the previous findings and is the, arguably non-surprising, finding that the focus in the sample companies' cyber risk disclosure is on positive aspects. More detail is provided regarding *risk mitigation* and how protected a company is, rather than regarding what might happen if the risk is realized. Amongst the companies reporting on cyber incidents, the focus is on what they have avoided rather than on providing more details on the incident themselves, or potential incidents which have not been adequately handled.

The fourth main finding concerns change. Over the three years, the companies change their reporting to varying degrees. No significant developments across the sample companies were noted but examining the companies individually revealed a few interesting changes. Iberdrola's cyber risk disclosures, for example, have increased in transparency and detail over the three years.

Lastly, compared to other companies, it is intriguing how little EnBW discloses on cyber risk. Institutional theory suggests that companies mimic their peers and follow the industry standard. Considering that all the companies examined are large, European-based and operating within one specific industry, it could be expected that EnBW would report on cyber risk in a similar way as the other four. Cyber risk is also of growing concern to business leaders worldwide and an issue which is of great concern to the energy industry. This raises the question of which influences and motivations lay behind EnBW's sparse cyber risk disclosures.

Overall, the findings of this study largely align with the theoretical perspective, proprietary cost theory and institutional theory, and previous research in general. The quality of cyber risk disclosures in the electric utility companies examined is mixed and there is room for improvement. The reporting on cyber incidents varies between companies even as cyber risk

has been acknowledged as a significant risk by all companies. The information included in the cyber risk disclosure is rather general and lacks details.

## 5.2 Practical Implications

In various ways, this thesis contributes to fulfilling some of the knowledge gaps in cyber risk reporting research. Contrary to the prominent US-focus in the existing English-language research within the subject matter, the companies examined here have their home countries in Europe. Furthermore, this study has highlighted the electric utility industry which is particularly vulnerable to cyber risks. Accordingly, the findings have contributed to the research area.

Because of these reasons, there are practical implications following from the results of this study. The analysis can be of use in the development of legislation and incentives in the area of corporate reporting and specifically cyber risk reporting. The findings provide a better understanding of the current state of cyber risk reporting of large international electric utility companies, and there appears to be room for improvement. However, despite the lack of legislation explicitly requiring cyber risk reporting, all the companies recognize cyber risk among the risk factors. Although generalizations cannot be made to larger populations, the authors believe that the close examination of the five companies over three years presents intriguing insights and a start for further discussion.

Yet, it is recognized that the ideal cyber risk reporting practice is far more complex than it appeared from the outset. It is challenging to design legislation or incentives that encourage truthful, material, substantive reporting. The fact that full legal compliance is not always the case further implies that it might be more useful to first approach the issue in terms of incentives and then review how these may be supported and strengthened through legislation. There is also the question of how much can be regulated or incentivized to not leave the companies too exposed regarding their cyber risk management. Despite these complex issues, this thesis certainly brings forth interesting insights.

Furthermore, the findings can be of interest to practitioners of cyber risk reporting, i.e., businesses. Due to the nature of the analysis, this thesis considers what can be viewed as good quality reporting. Consequently, the conclusions can demonstrate areas in which companies can improve their disclosure practices and matters which to focus on. However, the above-mentioned fine balance between transparency and vulnerability is also a crucial matter for practitioners.

## 5.3 Future Research

In light of the findings of this thesis, numerous future research avenues emerge. This section revolves around these avenues and proposes directions for further research. It includes both

suggestions regarding continued research on the specific questions examined in this thesis and suggestions for research within the same topic on adjacent issues.

Firstly, the themes identified in the cyber risk disclosures of the sample companies in this study would be useful in further cyber risk disclosure research. To see how they hold up and test their wider applicability it would be interesting to investigate whether they would emerge in a similar study with a larger sample size. This could potentially make way for more widespread generalizations of these themes. Performing further research on a larger pool of data could further also result in valuable additions or changes to the themes identified in this study. This could facilitate further research into the content of cyber risk reporting and capture further nuances of the data. The findings of this thesis could also be contrasted with an examination of smaller companies. Previous research illustrates company size to be a factor affecting risk reporting, and this study has focused on the cyber risk reporting practices of large companies.

Another possibility would be to examine a longer time period. Three years is a relatively short period and it can be difficult to notice trends that evolve slowly. Connected to this, it would be intriguing to see when cyber risk reporting has started and how it has evolved over the years up to this date. Such research avenues would complement the findings presented in this thesis.

Furthermore, since here the focus is on European-based companies and, to the knowledge of the authors of this thesis, most English-language research highlights cyber risk reporting among companies listed in the US, examining companies in other parts of the world would provide new insights. For example, what and how are Asian companies reporting on cyber risk? Relatedly, country-specific studies (other than the US) would contribute to expanding the knowledge frontier.

This thesis has limited the focus to cyber risk reporting only. To gain further insights, future research could examine cyber risk reporting practices relative to other risk factor disclosures. How material is cyber risk compared to other risks? To what extent do companies emphasize it, or is it considered as minor?

Lastly, all these future research suggestions can be implemented in either the energy or electric utility industry context or, alternatively, the industry examined could be different. There are few industry-specific studies about cyber risk reporting, and although this thesis contributes to fulfilling that gap, much is still to be researched. Cyber risk is, after all, increasingly common in today's complex international business environment.

# References


Abraham, S. & Shrives, P.J. (2014). Improving the Relevance of Risk Factor Disclosure in Corporate Annual Reports, The British accounting review, vol. 46, no. 1, pp. 91-107, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 6 April 2021]

Adam-Müller, A.F.A. & Erkens, M.H.R. (2020) Risk Disclosure Noncompliance, Journal of Accounting and Public Policy, vol. 39, no. 3, Available through: LUSEM Library website: http://www.lusem.lu.se/library [Accessed 6 April 2021]

AGCS. (n.d.). Allianz Risk Barometer, Available online: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Bailey, T., Maruyama, A. & Wallance, D. (2020). The Energy-Sector Threat: How to address cybersecurity vulnerabilities, Available online: https://www.mckinsey.com/business-functions/risk/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities [Accessed 6 April 2021]

BBC. (2017). Ukraine Power Cut 'Was Cyber-Attack', 11 January, Available online: https://www.bbc.com/news/technology-38573074 [Accessed 28 April 2021]

Beretta, S. & Bozzolan, S. (2004). A Framework for the Analysis of Firm Risk Communication, The International Journal of Accounting, vol. 39, no. 3, pp. 265-288 Available through: http://www.lusem.lu.se/library [Accessed 10 April 2021]

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity Awareness and Market Valuations, Journal of Accounting and Public Policy, vol. 37, no. 6, pp. 508-526, Available through: LUSEM Library website: http://www.lusem.lu.se/library [Accessed 6 April 2021]

Bryman, A. & Bell, E. (2011). Business Research Methods, 3rd edn, New York: Oxford University Press

Chiu, C.L, Zhang, J., Li, M., Wei, S., Xu, S. & Chai, X. (2020). A Study of Environmental Disclosures Practices in Chinese Energy Industry, Asian Journal of Sustainability and Social Responsibility, vol. 5, no. 1, pp. 1-21, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 6 April 2021]

CPA Canada & EY. (2020). When the World is Evolving Faster by the Second, How Can Your Cybersecurity Keep up? Cybersecurity disclosure report May 2020, Available through: https://www.cpacanada.ca/en/business-and-accounting-resources/other-general-business-topics/information-management-and-technology/publications/cybersecurity-disclosure-study-key-highlights [Accessed 5 April 2021]

Daugherty, W. (2013). The Evolving Landscape of Cybersecurity Disclosures, Securities Litigation Journal, vol. 23, no. 3, pp. 6-11, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 6 April 2021]

Deloitte. (2016). Beneath the Surface of a Cyberattack: A deeper look at business impacts, Available online: https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html [Accessed 5 April 2021]

Deloitte. (2017). Cyber Reporting Survey [pdf], Available online: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/deloitte-uk-governance-in-focus-cyber-risk-reporting.pdf [Accessed 5 April 2021]

Deutsches Rechnungslegungs Standards Committee e.V. (n.d.). Gas 20 - Group Management Report, Available online: https://www.drsc.de/en/pronouncements/gas-20/ [Accessed 19 April 2021]

Directive 2013/34/EU of the European Parliament and of the Council, OJ L 182, 29.6.2013, p. 19, Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02013L0034-20141211 [Accessed 23 April 2021]

Directive 2014/95/EU of the European Parliament and of the Council, OJ L 330, 15.11.2014, pp. 1-9, Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0095 [Accessed 23 April 2021]

Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A. Welburn, J.W. & Winkelman, Z. (2018). Estimating the Global Cost of Cyber Risk: Methodology and examples, Available Online: https://www.rand.org/pubs/research_reports/RR2299.html [Accessed 5 April 2021]

Dumay, J. (2016). A Critical Reflection on the Future of Intellectual Capital: From reporting to disclosure, Journal of Intellectual Capital, vol. 17, no. 1, pp. 168-184, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 5 April 2021]

E-ISAC & SANS. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense use case, Available online: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf [Accessed 28 April 2021]

EDF. (2018). Reference Document 2017 Including the Annual Financial Report [pdf], Available online: https://www.edf.fr/en/the-edf-group/dedicated-sections/investors-shareholders/reference-documents [Accessed 16 April 2021]

EDF. (2020). 2019 Universal Registration Document [pdf], Available online: https://www.edf.fr/en/the-edf-group/dedicated-sections/investors-shareholders/reference-documents [Accessed 16 April 2021]

EECSP-Expert Group. (2017). Cyber Security in the Energy Sector: Recommendations for the European Commission on a European strategic framework and potential future

legislative acts for the energy sector [pdf], Available online: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf [Accessed 6 April 2021]

Eling, M. & Schnell, W. (2016). What Do We Know about Cyber Risk and Cyber Risk Insurance?, The Journal of Risk Finance, vol. 17, no. 5, pp. 474-491, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 5 April 2021]

Elshandidy, T., Shrives, P.J., Bamber, M. & Abraham, S. (2018). Risk reporting: A review of the literature and implications for future research, Journal of Accounting Literature, vol. 40, no. 1, pp. 54-82, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 6 April 2021]

EnBW. (2018). Integrated Annual report 2017 [pdf], Available online: https://www.enbw.com/company/investors/news-and-publications/publications/ [Accessed 16 April]

EnBW. (2019). Integrated Annual report 2018 Extended Version: Including the notes and the declaration of corporate management [pdf], Available online: https://www.enbw.com/company/investors/news-and-publications/publications/ [Accessed 16 April]

EnBW. (2020). Integrated Annual report 2019 Extended Version: Including the notes and the declaration of corporate management [pdf], Available online: https://www.enbw.com/company/investors/news-and-publications/publications/ [Accessed 16 April]

Enel. (2018). Seeding Energies: Consolidated Non-Financial Statement (NFS) prepared in accordance with Italian Legislative Decree 254/16 _year 2017 [pdf], Available online: https://www.enel.com/content/dam/enel-com/documenti/investitori/informazioni-finanziarie/2017/annuali/en/nfs_2017.pdf [Accessed 15 April 2021]

Enel. (2018). Seeding Energies: Sustainability report 2017 [pdf], Available online: https://www.enel.com/content/dam/enel-com/documenti/investitori/sostenibilita/2017/sustainability-report_2017.pdf [Accessed 15 April 2021]

Enel. (2019). Sustainability Report 2018 [pdf], Available online: https://www.enel.com/content/dam/enel-com/documenti/investitori/sostenibilita/2018/sustainability-report_2018.pdf [Accessed 15 April 2021]

EUR-Lex. (2021). Brexit: EU-UK relationship, Available online: https://eur-lex.europa.eu/content/news/Brexit-UK-withdrawal-from-the-eu.html [Accessed 14 May 2021]

European Commission. (n.d.). Company reporting, Available online: https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting_en [Accessed 23 April 2021]

EY. (2020). What Companies are Disclosing About Cybersecurity Risk and Oversight, Available online: https://www.ey.com/en_us/board-matters/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight [Accessed 5 April 2021]

Gao, L., Calderon, T.G. & Tang, F. (2020). Public Companies' Cybersecurity Risk Disclosures, International Journal of Accounting Information Systems, vol. 38, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 6 April 2021]

Ghio, A. & Verona, R. (2020). The Evolution of Corporate Disclosure: Insights on traditional and modern corporate communication, [e-book] Cham: Springer International Publishing, Available through: LUSEM University Library website http://www.lusem.lu.se/library [Accessed 7 April 2021]

Gonidakis, F.K., Koutoupis, A.G., Tsamis, A.D. & Agoraki, M.K. (2020). Risk Disclosure in Listed Greek Companies: The effects of the financial crisis, Accounting Research Journal, vol. 33, no. 4/5, pp. 615-633, Available through: LUSEM Library website: http://www.lusem.lu.se/library [Accessed 9 April 2021]

Graham, J.R., Campbell, H. R. & Rajgopal, S. (2005). The Economic Implications of Corporate Financial Reporting, working paper, no. 10550, National Bureau of Economic Research, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 6 April 2021]

CSR Europe, GRI & Accountancy Europe. (2018). Member State Implementation of EU NFI Directive, Available online: https://www.accountancyeurope.eu/publications/member-state-implementation-eu-nfi-directive/ [Accessed 23 April 2021]

Haapamäki, E. & Sihvonen, J. (2019). Cybersecurity in Accounting Research, Managerial Auditing Journal, vol. 34, no. 7, pp. 808-834, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 7 April 2021]

Haller, A., Link, M. & Groß, T. (2017). The Term 'Non-Financial Information': A semantic analysis of a key feature of current and future corporate reporting, Accounting in Europe, vol. 14, no. 3, pp. 407-429, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 5 April 2021]

Héroux, S. & Fortin, A. (2020). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index, Accounting perspectives, vol. 19, no. 2, pp. 73-100, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 7 April 2021]

Iberdrola. (2018). Annual Financial Report: Iberdrola, S.A. and subsidiaries / financial year 2017 [pdf], Available online: https://www.iberdrola.com/shareholders-investors/annual-reports [Accessed 16 April]

Iberdrola. (2020a). Annual Financial Report: Iberdrola, S.A., and subsidiary companies year 2019 [pdf], Available online: https://www.iberdrola.com/shareholders-investors/annual-reports [Accessed 16 April]

Iberdrola. (2020b). Statement of Non-Financial Information, Sustainability Report: Financial year 2019, Available online: https://www.iberdrola.com/shareholders-investors/annual-reports [Accessed 16 April]

ICAEW. (n.d.). Brexit and Financial Reporting, Available online: https://www.icaew.com/brexit/financial-reporting [Accessed 24 May 2021]

Investor.gov. (n.d.). Form 10-K, Available online: https://www.investor.gov/introduction-investing/investing-basics/glossary/form-10-k [Accessed 7 April 2021]

Julien, H. (2008). Content Analysis, in L.M. Given (ed), The SAGE Encyclopedia of Qualitative Research Methods, [e-book] Thousand Oaks: SAGE, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 15 April 2021]

Kelton, A.S. & Pennington, R.R. (2020). Do Voluntary Disclosures Mitigate the CyberSecurity Breach Contagion Effect?, Journal of Information Systems, vol. 34, no. 3, pp. 133-157, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 7 April 2021]

Kennedy, B.L. (2018). Deduction, Induction, and Abduction, in U. Flick (ed), The SAGE Handbook of Qualitative Data Collection, [e-book] London: SAGE Publications, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 19 April 2021]

Khandelwal, C., Kumar, S., Verma, D. & Singh, H.P. (2019). Financial risk reporting practices: Systematic literature review and research agenda, The Bottom Line, vol. 32, no. 3, pp. 185-210, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 6 April 2021]

Kuckartz, U. (2014). Qualitative Text Analysis: A Guide to Methods, Practice & Using Software, [e-book] Los Angeles: SAGE, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 6 April 2021]

Leopizzi, R., Iazzi, A., Venturelli, A. & Principale, S. (2020). Nonfinancial Risk Disclosure: The "state of the art" of Italian companies, Corporate Social Responsibility & Environmental Management, vol. 27, no. 1, pp. 358-368, Available through: LUSEM Library website: http://www.lusem.lu.se/library [Accessed 10 April 2021]

Li, H., No, W.G. & Wang, T. (2018). SEC's Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors, International Journal of Accounting Information Systems, vol. 30, pp. 40-55, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 7 April 2021]

Linsey, P.M. & Shrives, P.J. (2006). Risk Reporting: A study of risk disclosures in the annual reports of UK companies, The British Accounting Review, vol. 38, no. 4, pp. 387-404, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 5 April 2021]

Mason, J. (2002). Qualitative Researching, 2nd edn, London: SAGE Publications

Mazumder, M. & Hossain, D.M. (2018). Research on Corporate Risk Reporting: Current trends and future avenues, Journal of Asian Finance, Economics and Business, vol. 5, no. 1, pp. 29-41, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 5 April 2021]

Microsoft. (2019). Overview of the Marsh-Microsoft 2019 Global Cyber Risk Perception survey results, Available online: https://www.microsoft.com/security/blog/2019/09/18/marsh-microsoft-2019-global-cyber-risk-perception-survey-results/ [Accessed 5 April 2021]

Morse, E.A., Raval, V. & Wingender, J.R. Jr. (2017). SEC Cybersecurity Guidelines: Insights into the utility of risk factor disclosures for investors, The Business Lawyer, vol. 73, no. 1, pp. 1-34, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 6 April 2021]

Nicolo, G., Zanellato, G., Manes-Rossi, F. & Tiron-Tudor, A. (2021). Corporate Reporting Metamorphosis: Empirical findings from state-owned enterprises, Public Money & Management, vol. 41, no. 2, pp. 138–147, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 19 April 2021]

OECD. (2015). OECD Guidelines on Corporate Governance of State-Owned Enterprises: 2015 edition, Paris: OECD Publishing, Available online: http://dx.doi.org/10.1787/9789264244160-en [Accessed 19 April 2021]

Onoja, A. & Agada, G.O. (2015). Voluntary Risk Disclosure in Corporate Annual Reports: An empirical review, Research Journal of Finance and Accounting, vol. 6, no. 17, Available online: https://core.ac.uk/download/pdf/234631005.pdf [Accessed 5 April 2021]

Pooser, D.M., Browne, M.J. & Arkhangelska, O. (2018). Growth in the Perception of Cyber Risk: Evidence from US P&C insurers, The Geneva Papers on Risk and Insurance-Issues and Practice, vol. 43, no. 2, pp. 208-223, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 6 April 2021]

Radu, C. & Smaili, N. (2021). Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from cybersecurity related disclosure, Journal of Business Ethics, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 5 April 2021]

Raquiba, H. & Ishak, Z. (2019). Sustainability Reporting Practices in the Energy Sector of Bangladesh, International Journal of Energy Economics and Policy, vol. 10, no. 1, pp.

508-516, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 6 April 2021]

Saunders, M., Lewis, P. & Thornhill, A. (2007). Research Methods for Business Students, 4th edition, Harlow: Pearson Education Limited, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 19 April 2021]

SSE. (2018). Creating Value in a Sustainable Way: SSE plc Annual Report 2018 [pdf], Available online: https://www.sse.com/investors/reports-and-results/ [Accessed 16 April 2021]

S&P Global. (n.d.a). Top 250 Global Energy Company Rankings: 2020, Available online: https://www.spglobal.com/platts/top250/rankings/2020 [Accessed 13 April 2021]

S&P Global. (n.d.b). Top 250 Global Energy Company Rankings: Methodology, Available online: https://www.spglobal.com/platts/top250/methodology [Accessed 13 April 2021]

Skinner, C.P. (2019). Bank Disclosures of Cyber Security, Iowa Law Review, vol. 105, no. 1, pp. 239-281, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 5 April 2021]

Slacik, J. & Greiling, D. (2019). Compliance with Materiality in G4-Sustainability Reports by Electric Utilities, International Journal of Energy Sector Management, vol. 14, no. 3, pp. 582-608, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 6 April 2021]

Spanos, G. & Angelis, L. (2016). The Impact of Information Security Events to the Stock Market: A systematic literature review, Computers & Security, vol. 58, pp. 216-229, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 5 April 2021]

Ştefănescu, C.A., Tiron-Tudor, A. & Moise, E.M. (2021). EU Non-Financial Reporting Research: Insights, gaps, patterns and future agenda, Journal of Business Economics and Management, vol. 22, no. 1, pp. 257-276, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 28 April 2021]

Strupczewski, G. (2021). Defining Cyber Risk, Safety Science, vol. 135, pp. 105-143, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 5 April 2021]

Talbot, D. & Boiral, O. (2018). GHG Reporting and Impression Management: An assessment of sustainability reports from the energy sector, Journal of Business Ethics, vol. 147, no. 2, pp. 367-383, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 6 April 2021]

Traxler, A.A. & Greiling, D. (2019). Sustainable Public Value Reporting of Electric Utilities, Baltic Journal of Management, vol. 14, no. 1, pp. 103-121, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 6 April 2021]

United Nations. (2017). The Role of Disclosure in Risk Assessment and Enhancing the Usefulness of Corporate Reporting in Decision-Making: Note by the UNCTAD secretariat [pdf], Available online: https://unctad.org/system/files/official-document/ciiisard82_en.pdf [Accessed 5 April 2021]

Veltri, S. (2020). Mandatory Non-Financial Risk-Related Disclosure, [e-book] Cham: Springer International Publishing, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 5 April 2021]

Verizon. (2020). 2020 Data Breach Investigations Report, Available online: https://enterprise.verizon.com/resources/reports/dbir/2020/smb-data-breaches-deep-dive/ [Accessed 5 April 2021]

Wei, L., Li, G., Zhu, X., Sun, X. & Li, J. (2019). Developing a Hierarchical System for Energy Corporate Risk Factors Based on Textual Risk Disclosures, Energy Economics, vol. 80, pp. 452-460, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 6 April 2021]

Williamson, K., Given L. M. & Scifleet, P. (2018). Qualitative Data Analysis, in Williamson, K. & Johanson, G. (eds), Research Methods: Information, systems, and contexts, pp. 453-476, Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 16 April 2021]

Wong, J. C. & Solon, O. (2017). Massive Ransomware Cyber-Attack Hits Nearly 100 Countries Around the World, The Guardian, 12 May, Available online: https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs [Accessed 4 May 2021]

World Economic Forum. (2019). Regional Risks for Doing Business 2019, Available online: https://www.weforum.org/reports/regional-risks-for-doing-business-2019 [Accessed 5 April 2021]

# Appendix A

Passages from the EU directives discussed in Section 2.3

| Directive | Main relevant passages |
|---|---|
| 2013/34/EU | **Article 19(1-2): Contents of the management report**<br><br>"1. The management report shall include a fair review of the development and performance of the undertaking's business and of its position, together with a description of the principal risks and uncertainties that it faces.<br><br>The review shall be a balanced and comprehensive analysis of the development and performance of the undertaking's business and of its position, consistent with the size and complexity of the business.<br><br>To the extent necessary for an understanding of the undertaking's development, performance or position, the analysis shall include both financial and, where appropriate, non-financial key performance indicators relevant to the particular business, including information relating to environmental and employee matters. In providing the analysis, the management report shall, where appropriate, include references to, and additional explanations of, amounts reported in the annual financial statements.<br><br>2. The management report shall also give an indication of:<br><br>(a) the undertaking's likely future development;<br><br>(b) activities in the field of research and development;<br><br>(c) the information concerning acquisitions of own shares prescribed by Article 24(2) of Directive 2012/30/EU;<br><br>(d) the existence of branches of the undertaking; and<br><br>(e) in relation to the undertaking's use of financial instruments and where material for the assessment of its assets, liabilities, financial position and profit or loss:<br><br>(i) the undertaking's financial risk management objectives and policies, including its policy for hedging each major type of forecasted transaction for which hedge accounting is used; and |

| | |
|---|---|
| | (ii) the undertaking's exposure to price risk, credit risk, liquidity risk and cash flow risk.” |
| 2013/34/EU | **Article 29(1): The consolidated management report**<br><br>“1. The consolidated management report shall, as a minimum, in addition to any other information required under other provisions of this Directive, set out the information required by Articles 19 and 20, taking account of the essential adjustments resulting from the particular characteristics of a consolidated management report as compared to a management report in a way which facilitates the assessment of the position of the undertakings included in the consolidation taken as a whole.” |
| 2014/95/EU | **Article 19a(1): Non-financial statement**<br><br>“1. Large undertakings which are public-interest entities exceeding on their balance sheet dates the criterion of the average number of 500 employees during the financial year shall include in the management report a non-financial statement containing information to the extent necessary for an understanding of the undertaking's development, performance, position and impact of its activity, relating to, as a minimum, environmental, social and employee matters, respect for human rights, anti-corruption and bribery matters, including:<br><br>(a) a brief description of the undertaking's business model;<br><br>(b) a description of the policies pursued by the undertaking in relation to those matters, including due diligence processes implemented;<br><br>(c) the outcome of those policies;<br><br>(d) the principal risks related to those matters linked to the undertaking's operations including, where relevant and proportionate, its business relationships, products or services which are likely to cause adverse impacts in those areas, and how the undertaking manages those risks;<br><br>(e) non-financial key performance indicators relevant to the particular business.<br><br>Where the undertaking does not pursue policies in relation to one or more of those matters, the non-financial statement shall provide a clear and reasoned explanation for not doing so. |

| | |
|---|---|
| | The non-financial statement referred to in the first subparagraph shall also, where appropriate, include references to, and additional explanations of, amounts reported in the annual financial statements.<br><br>Member States may allow information relating to impending developments or matters in the course of negotiation to be omitted in exceptional cases where, in the duly justified opinion of the members of the administrative, management and supervisory bodies, acting within the competences assigned to them by national law and having collective responsibility for that opinion, the disclosure of such information would be seriously prejudicial to the commercial position of the undertaking, provided that such omission does not prevent a fair and balanced understanding of the undertaking's development, performance, position and impact of its activity.<br><br>In requiring the disclosure of the information referred to in the first subparagraph, Member States shall provide that undertakings may rely on national, Union-based or international frameworks, and if they do so, undertakings shall specify which frameworks they have relied upon." |
| 2014/95/EU | **Article 29a(1): Consolidated non-financial statement**<br><br>"1. Public-interest entities which are parent undertakings of a large group exceeding on its balance sheet dates, on a consolidated basis, the criterion of the average number of 500 employees during the financial year shall include in the consolidated management report a consolidated non-financial statement containing information to the extent necessary for an understanding of the group's development, performance, position and impact of its activity, relating to, as a minimum, environmental, social and employee matters, respect for human rights, anti-corruption and bribery matters, including:<br><br>(a) a brief description of the group's business model;<br><br>(b) a description of the policies pursued by the group in relation to those matters, including due diligence processes implemented;<br><br>(c) the outcome of those policies;<br><br>(d) the principal risks related to those matters linked to the group's operations including, where relevant and proportionate, its business relationships, products or services which are likely to cause adverse impacts in those areas, and how the group manages those risks;<br><br>(e) non-financial key performance indicators relevant to the particular business. |

| | |
|---|---|
| | Where the group does not pursue policies in relation to one or more of those matters, the consolidated non-financial statement shall provide a clear and reasoned explanation for not doing so.<br><br>The consolidated non-financial statement referred to in the first subparagraph shall also, where appropriate, include references to, and additional explanations of, amounts reported in the consolidated financial statements.<br><br>Member States may allow information relating to impending developments or matters in the course of negotiation to be omitted in exceptional cases where, in the duly justified opinion of the members of the administrative, management and supervisory bodies, acting within the competences assigned to them by national law and having collective responsibility for that opinion, the disclosure of such information would be seriously prejudicial to the commercial position of the group, provided that such omission does not prevent a fair and balanced understanding of the group's development, performance, position and impact of its activity.<br><br>In requiring the disclosure of the information referred to in the first subparagraph, Member States shall provide that the parent undertaking may rely on national, Union-based or international frameworks, and if it does so, the parent undertaking shall specify which frameworks it has relied upon.” |

# Appendix B

Selected sample companies and the annual reports/publications used for data collection

| **Company** | **Annual publications** |
|---|---|
| Electricité de France | Reference/Universal registration document<br>Management report<br>Consolidated financial statements |
| Iberdrola | Integrated report<br>Annual financial report<br>Sustainability report<br>Annual corporate governance report |
| Enel | Annual report<br>Consolidated non-financial statement<br>Sustainability report |
| SSE | Annual report<br>Risk report<br>Full year result statement<br>Sustainability report |
| EnWB Energie Baden-Württemberg | Integrated annual report<br>Financial statements (AG when consolidated was not available)<br>Corporate governance report |

# Appendix C

List of keywords used for collecting data from annual reports, adapted from Li, No and Wang (2018)

| |
|---|
| (information\|network\|computer) security |
| confidential data |
| confidentiality of data |
| corruption of data |
| cyber |
| data breach |
| data confidentiality |
| data corruption |
| data theft |
| encryption |
| hacking\|hacker |
| information technology (security\|attack) |
| malware |
| phishing |
| ransomware |

# Appendix D

Themes identified in the companies' cyber risk reporting

**bolded** = main themes
*italics* = sub-themes of the main theme above

| Theme | Meaning |
|---|---|
| **Risk types** | **Certain types of cyber risk** |
| **Risk consequences** | **Potential or realized consequences of cyber risks** |
| *Magnitude of impact* | Size or magnitude of potential or actual impact |
| *Specified type* | Specification of the type of consequence |
| *Company focus* | Consequences affecting the company |
| *Stakeholder focus* | Consequences affecting specific stakeholders |
| **Risk mitigation** | **Reduction/minimization of cyber risk or the impact of cyber risk** |
| *Prevention* | Preventing the realization of cyber risk |
| *Reduction of impact* | Reducing the impact of a realized cyber risk |
| *Mitigation fallibility* | Weaknesses of the risk mitigation |
| **Cyber incidents** | **Cyber incidents that have occurred** |
| *Everyday incidents* | Smaller incidents with a lower (potential) impact |
| *Significant events* | Larger events with a higher (potential) impact |

| **Information scope** | **Information pertaining to the company or to companies in general** |
|---|---|
| *Company-specific information* | Information pertaining to the company |
| *General information* | Information regarding all companies or all companies in the industry |
| **Time orientation** | **The focus is on the past or the future** |
| *Past time orientation* | Past actions or occurrences |
| *Future time orientation* | Future intentions, goals and plans |
| **Time relevance of the risk** | **Explanation of why the cyber risk has been or is relevant** |
| *Past year relevance* | Explanation of why the cyber risk has been relevant the past year |
| *Future relevance* | Explanation of why the cyber risk is relevant for the future |
| **Vagueness** | **Few details and short explanations** |