PhD in Business // No. 94 - 2022

From intangibility to 'fluid' tangibility of cyberrisk: localisation, visualisation, and prevention

Silje Aakre

NORD UNIVERSITY BUSINESS SCHOOL

NORD University

www.nord.no

From intangibility to ‘fluid’ tangibility of cyberrisk: localisation, visualisation, and prevention

Silje Aakre

PhD in Business
Nord University Business School

PhD in Business no. 94 (2022)
From intangibility to 'fluid' tangibility of cyberrisk: localisation, visualisation, and prevention
Silje Aakre

ISBN: 978-82-92893-84-5
ISSN: 2464-4331

Print: Trykkeriet NORD

Nord University
N-8049 Bodø
Tel: +47 75 51 72 00
www.nord.no

ACKNOWLEDGEMENTS

In our digitalised world, something and someone are always fighting for our time and attention. I would like to take this opportunity to express my gratitude towards those who devoted time and attention to this PhD project – as peers and academics, as interviewees and stakeholders, as colleagues and supervisors, as nearest and dearest.

Thank you, Anatoli Bourmistrov, for your constructive feedback and for inspiring me with your solution-oriented approach. Parallel to the PhD project, I have conceptualised a phenomenon I call 'the Anatoli effect'. The phenomenon explains the experience of, in general, feeling better and more optimistic after supervision meetings, and is acknowledged among my peers.

Thank you, Jan Mouritsen, for welcoming me to CBS where I grew as a researcher. I am particularly grateful for your supervision towards and through the finalising steps in the PhD dissertation. I appreciate your friendly suggestions to always explore how everything can be taken one step further.

Special thanks to Eva Brekka and NC-Spectrum for aiding me with the 'Pippi attitude' that anything can be done, investing in me, and allocating the time, resources and network to pursue this PhD.

Finally, one of the great perks of being an industrial researcher has been my three places of residence: Nord university business school in Bodø, Copenhagen business school Department of operations management, and NC-Spectrum in Kviteseid. I am privileged to have you all as colleagues.

Frederiksberg, 09.06.2022

Silje Aakre

ABSTRACT

In a digitalised and globalised world, cyberrisk has become a key concern for organisations. The challenge is that global cyberrisk is intangible – almost like gas – something that cannot be discerned in the traditional way, but which can cause fatal consequences. To avoid being trapped in a paralysed state of unknowing, we need theory to interpret cyberrisk, and perspectives to intervene with the intangibility. This dissertation applies Beck's risk society thesis, and asks: *what challenges does the intangibility of cyberrisk represent for organisations, and how can they mitigate the intangibility of cyberrisk?*

The intangibility of cyberrisk is studied by applying Giddens' understanding of manufactured risks, and by extending Beck's typology and features of global manufactured risks in the risk society. The dissertation argues that cyberrisk is the archetype of global risks, and therefore by its very nature, intangible. Four perspectives on cyberrisk are studied in the incorporated articles addressing regulations, openness, foresight, and strategy. These four perspectives allow us to intervene with intangibility. Cyberrisk can be *localised* by approaches to assess its manifested and imagined consequences. It can be *visualised* to allow for a more meaningful discussion of cyberrisk, and consequently, *prevented*. This way, cyberrisk no longer remains in a gas state, but can become 'fluid' and thus, more tangible allowing for mitigation.

In addition to the individual contributions of research articles incorporated into this dissertation, the overarching discussions synthesizing them as a whole makes contributions to the (world) risk society thesis. It achieves this by extending Beck's typology of global risks and elaborating on the role and magnitude of cyberrisk in the risk society. Finally, this dissertation highlights the intangibility of cyberrisk in a managerial context and suggests perspectives and strategies to interpret and mitigate intangible cyberrisk.

SAMMENDRAG

I en verden preget av digitalisering og globalisering, har cyberrisiko blitt en stadig mer sentral utfordring for organisasjoner. Utfordringen er at global cyberrisko er uhåndgripelig – nesten som gass – noe vi ikke kan sanse i tradisjonell forstand, men som likevel kan få fatale følger. For å unngå å bli handlingslammet i en tilstand av uvisshet, trenger vi teori for å forstå cyberrisiko, og perspektiver til å gripe inn i det uhåndgripelige. Denne avhandlingen anvender det teoretiske rammeverket fra risikosamfunnet, og spør: *Hvilke utfordringer representerer uhåndgripelig cyberrisiko for organisasjoner, og hvordan kan de håndtere den?*

Avhandlingen anvender Giddens' forståelse av fabrikkert (menneskeskapt) risiko, og utvider Becks typologi og kjennetegn ved uhåndgripelig risiko. Den plasserer cyberrisiko som arketypen av global risiko i risikosamfunnet, noe som betyr at cyberrisiko av natur er uhåndgripelig. Dette studeres ved hjelp av fire perspektiver fra avhandlingens artikler: Regulering, åpenhet, framsyn og strategi. Perspektivene tillater oss å redusere uhåndgripeligheten knyttet til cyberrisiko. Cyberrisiko kan *lokaliseres* ved å studere faktiske og mulige konsekvenser. Den kan *visualiseres* for å legge til rette for mer meningsfulle diskusjoner og forståelse av cyberrisiko, og som resultat kan cyberrisiko *forebygges*. Dette medfører at cyberrisiko ikke lenger er som gass, men i en noe mer håndfast form som gjør det mulig å redusere risiko.

Utover de individuelle bidragene i avhandlingens forskningsartikler, bidrar avhandlingen i sin helhet ved å videreutvikle Becks typologi over globale risikoer og utdype rollen til og viktigheten av cyberrisiko i (verdens-)risikosamfunnet. I tillegg framhever avhandlingen hvordan uhåndgripelig cyberrisiko kan forstås og håndteres i organisasjoner.

CONTENTS

TABLES

FIGURES

DISSERTATION ARTICLES

Article 1: Aakre, S. (2020). "Just tell us what to do" Regulations and cyber risk appetite in the electric power industry. In P. Baraldi, F. Di Maio, & E. Zio (Eds.), *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*. Research Publishing, Singapore.

Article 2: Aakre, S. (2020). Hvilket trusselbilde står norske virksomheter overfor, og hvordan kan åpenhet bidra til å forstå cyberrisiko? *Magma, 20*(2), 18–26.

Article 3: Bourmistrov, A. & Aakre, S. (2020). Framsyn som risikoradar: Hvordan kan scenarioanalyse forbedre cybersikkerhet? *Magma, 20*(2), 55–61.

Article 4: Aakre, S. (2022, preprint). Ransomware as business models.

1 INTRODUCTION

Imagine a cross-sectional pause in Mary Wollstonecraft Shelley's novel, *Frankenstein,* in the moment where the scientist Victor Frankenstein is about to take the final step in his attempt to create artificial life:

> *"It was one o'clock in the morning. The rain fell against the window. My candle was nearly burned out. I put together the instruments, so I could give life to the thing on my table"* (Shelley, 1818/2020: 32)

Imagine Frankenstein using this moment to reflect on his achievement and its potential effects: 'what might be the consequences to him, and to the world? Today and to future generations? How can its effects be interpreted and comprehended? Is he responsible for the potential ramifications? Can he control the effects, and can negative consequences be prevented? If so, how can he know which interventions are needed?'. Imagine society being 'trapped' in this reflexive state of unknowing and anticipation of future risk. This reflexive state is where the risk society begins. How it begins is through our technological creations and the side effects we cannot control. And where it ends may be the death of the creator.

The risk society thesis has gained influence in terms of how risk is defined, as well as how societal development can be explained. The theory suggests that we are experiencing the 'end' of the industrial society, and are moving towards a risk society where risks are gaining increasing attention and importance (Beck, 1992b). This is because the concept of risk has changed, not because it is a new concept. Life on earth has always been characterised by possible dangers as well as more favourable outcomes. Christopher Columbus' voyage reached America, although, being lost at sea or being attacked by pirates could have been more likely alternatives. Seafaring is indeed often attributed as the origin of the risk term (de Caprona, 2013: 1214-1215; Ewald, 1993: 226), but as we shall see, the dominating risks in our time are fundamentally different from those of Columbus' time. Risk changed when we became

aware that our own technological advancements caused ripple effects which years later spun into risks we did not foresee. Risk changed when *we* became the mother of risk.

While 'old' risks are experienced as external and originating from the outside, 'new' risks are manufactured, and understood as consequences of human activity (Giddens, 2002: 26). The 'irony' of new risks in the risk society (Beck, 2006: 329) is that they can be attributed to the unintended ripple effects of techno-scientific achievements (Ekberg, 2007: 348). As such, risk becomes the ripple effect of success. Since the risk society thesis was published by Ulrich Beck in 1986, it has been debated, developed, and applied to explain the 'irony' of success and disaster. Because we succeeded in producing nuclear power for generating electricity, risks associated with nuclear disasters, such as the Chornobyl accident, are a concern (Beck, 1986: 8). It is this notion of self-inflicted risk that makes the risk society "increasingly occupied with debating, preventing and managing risks that it itself has produced" (Beck, 2006: 332). In later years, the risk society thesis was further developed and adapted to address other global and (re-)emerging risks and tendencies in society, such as financial crises (Curran, 2015), terrorism (Aradau & van Munster, 2007; Beck, 2002) and cyberrisk (van Loon, 2000, 2002; Lupton, 2016).

The influence of digital technologies in society makes cyberrisk a natural and needed extension of Beck's analysis of the risk society (van Loon, 2000, 2002: 158; Lupton, 2016). Beck himself, only briefly addressed issues such as digital freedom risk, but strongly emphasised their importance (Beck, 2013). Digital technologies have influenced the risk society by the ways in which risks are produced (van Loon, 2000) and reproduced digitally, like they are through social media (Lupton, 2016). Hence, cyberrisk is not only an effect of digital technologies, but digital technologies also mediate risk. Cyberrisk can therefore expand in two dimensions, as self-replication actors such as viruses (van Loon, 2002), and through human encounters with cyberrisk (Lupton, 2016). The Internet allows users to act as 'prosumers', to produce and consume content

and challenge media's traditional representation of risk (Lupton, 2016: 304). However, the numerous sources and the volume of content, brings new challenges of surveillance and self-surveillance, misinformation, and 'fake news'.

Intangibility of risk

Our digitalised society makes cyberrisk the archetype of manufactured risks in our time. The emergence of the Internet and the success in connecting 'everyone to everyone, and everything to everything', drives benefits and risks simultaneously. Cyberrisk is global and intangible. Intangibility of cyberrisk can be found in the complexity of changing contexts, multiple actors, uncertainty about its effects (Pentland, 2016: 198), the "iceberg character" of incidents (Smidt & Botzen, 2018: 241), and the divergent terminology and definitions (Ramirez & Choucri, 2016; Strupczewski, 2021). Moreover, the interdependence between benefits and risks of digitalisation can be challenging to anticipate, interpret, and understand (Pentland, 2016: 193). Intangibility is therefore not only a challenge in the risk society thesis, but also a characteristic of cyberrisk.

Besides addressing the challenges of limited knowledge for assessing cyberrisk (Kosub, 2015; Marotta & McShane, 2018), few seem to devote attention to exploring the intangibility of cyberrisk or to how the intangibility of risk can be mitigated. Cyberrisk as a field is relatively new (Strupczewski, 2021: 9), and literature from computer science has contributed to its growth over the last decade (Eling & Schnell, 2016). As a result, technical solutions to identify, assess and manage risk have been given the broadest attention (see e.g., Cherdantseva et al., 2016; Paté-Cornell et al., 2018,). However, a majority of this literature fail to consider uncertainty, which is a critical element of risk (Scala et al, 2019: 2021). In addition to the technological perspective on cyberrisk, scholars have studied cyberrisk from an insurance perspective and problematised the challenges of calculating risk and establishing an insurance market (see e.g., Eling & Wirfs, 2019: 1118; Peters et al., 2018). A third perspective in the literature can be classified as a more general (risk) management perspective with

special attention to risk management frameworks (see e.g., Kosub, 2015). However, traditional risk management is also criticised, and found to be insufficient in managing cyberrisk (Eling et al., 2021; Marotta & McShane, 2018), especially when faced with intangible cyberrisk, such as 'black swans' (Aakre, 2020a; Bourmistrov & Aakre, 2020; Refsdal et al., 2015: 123-124).

A central problem to interpret, and manage manufactured risks, is their intangibility. This means that we struggle to understand them. Intangibility is an important conceptual problem in the risk society thesis because it challenges the fundamental idea and understanding of risk and the risk society. The intangibility of manufactured risks is characterised by the three interconnected features of de-localisation, incalculability, and non-compensability (Beck, 2009a: 52-54). To exemplify this: climate change is borderless and has a long latency; therefore, it is de-localised. Because we struggle to foresee its risks and their consequences, it is incalculable. This, combined with consequences that can threaten human life, make climate change non-compensable. The intangibility related to manufactured risks can be described as a state of 'non-knowledge' (Beck, 2009a: 115). The intangibility is argued to resemble pure uncertainty, unknown unknowns, and a 'non-knowledge society', rather than risk and a risk society (Gross, 2016: 397-398). Additionally, the 'complete' intangibility of manufactured risks is clearly a profound challenge for organisations and authorities tasked with assessing and managing risk.

Aim and significance

While sociology offers rich explanations for the problematisation of risk, it offers limited, if any solutions for how to manage or navigate risk at the organisational level. Metaphorically speaking, manufactured risks are like gases, moving and expanding. Risk at a gas state can hardly be sensed in the traditional sense, but only discerned by its consequences. The difficulty in sensing the risks makes them 'omnipresent', as we cannot know how, where, and when they might manifest themselves. Risk in a gas state indicates that containing the risk is challenging, and consequently that society

and organisations need to always be alert. This is clearly challenging, or impossible in practice. For management purposes, risks should preferably resemble a solid state. Solid has a constant shape and volume which can be observed and measured with high reliability. Risk at a solid state represents tangibility. An example of this is the reliable estimate of turnover in the next quarter, or which machine in the production line is likely to need spare parts in the near future. Risk at a solid state allows managers to intervene and mitigate risk, and thereby show actions and results. When risk is at a gas state, management is more of an act of fumbling in the dark. It is impossible to know which levers are available, which levers to pull, and what the effect might be. The critical lack of knowledge leaves the manufactured risks at the intangible gas state. The question is whether it is possible, both for theoretical and practical purposes, to interpret this intangibility, and to mitigate manufactured risks. The overall research question of this dissertation is therefore: *what challenges does the intangibility of cyberrisk represent for organisations, and how can they mitigate the intangibility of cyberrisk?*

The intangibility of cyberrisk is a crucial challenge for management. For how can we asses an event that we do not know where, what, how, when, or if will occur, and offer guidance for its risk mitigation? Is it possible to become familiar with the intangible gas of cyberrisk, and foresee the consequences before Frankenstein's creation approaches us?

This dissertation applies Beck's (2009a: 52-54) three features of intangibility: de-localisation, incalculability, and non-compensability. These features of intangibility are discussed in relation to cyberrisk. In this way, the dissertation develops the role and implications of cyberrisk in the risk society further (van Loon, 2000, 2002; Lupton, 2016). The discussion is based on the four integral articles in this dissertation which explore how organisations may gain knowledge, explore unknown unknowns, and improve management of cyberrisk. The articles explore cyberrisk through the four different perspectives of: regulations, openness, foresight, and strategy. Because the risk is 'omnipresent', the perspectives are chosen to show different cyberrisk situations,

where the aim is to assess intangible cyberrisk. This sheds light on the role of knowledge (Sørensen, 2018: 10-11) and the problem of complete intangibility and 'non-knowledge' (Gross, 2016) in the risk society.

The dissertation extends Beck's typology of global manufactured risks (Beck, 2009a: 13-14), to include the archetype of risk in our time, cyberrisk. The discussion and comparison will show that cyberrisk is more comprehensive and multisided than comparable risks in the risk society. While other scholars have problematised the intangibility of risks caused by the lack of knowledge (and therefore the risk society thesis), this dissertation investigates the features of intangibility, and explores how we can mitigate the intangibility of cyberrisk. The discussions raise several questions such as: 'can we *localise* cyberrisk? Can we gain knowledge about cyberrisk through different means or a broader understanding of calculation, such as *visualisation*? And lastly, if risks cannot be compensated, how can cyberrisk be *prevented*?'. The work shows paths to gain knowledge about complex and intangible cyberrisk and argues that it is possible to explore and demystify cyberrisk, even unknown unknowns. To return to our metaphor of risk as gas and solid, this dissertation acknowledges that it cannot fulfil the 'management dream' of a solid state of cyberrisk. Instead, we may manage to turn risks into a 'fluid' – and thus more tangible – state.

Structure of the dissertation

The second chapter of this dissertation outlines the theoretical basis of the risk society with attention to the logic of manufactured risks and the three features of intangibility, to show how global risks become a crucial challenge for management. The third chapter covers methodology, elaborating on how the perspectives in the articles were motivated through a 'journey of discoveries', and how they shaped the dissertation. This chapter also addresses the philosophical stance, an overview of the data and its analysis across the individual articles, as well as reflections on the role of an industrial researcher and ethical considerations. Chapter four offers a brief overview of the four incorporated articles in the dissertation. The discussions in the fifth chapter, connect

the four articles on cyberrisk to the broader perspective of global manufactured risks and the features of intangibility. These discussions address how cyberrisk is more complex than global manufactured risks of comparable importance, and how intangibility can be challenged and mitigated through localisation, visualisation, and prevention. The fifth chapter ends with a summary and an outline of the dissertation's contributions. To conclude, the sixth chapter revisits the research question and presents an encompassing summary of the dissertation.

2 THEORETICAL FRAMEWORK

To explore the intangible nature of global cyberrisk, it is imperative to discuss the risk society thesis. This is addressed with particular attention to manufactured risks in section 2.1, intangibility of global risks in section 2.2, and how intangible risks becomes a challenge for management in section 2.3. The chapter then presents an overview of the theoretical framework for the dissertation as a whole.

2.1 Risk society and manufactured risks

The term 'risk society' (Risikogesellschaft) was coined by the German sociologist Ulrich Beck in his 1986 book (Beck, 1986). The risk society thesis succeeded in tapping into important tendencies at the time concerning nuclear power, climate change, distrust of expert systems, and a failure of regulatory institutions to manage major risks (Mythen, 2021: 535). In terms of impact, the book was published at a 'fortunate' time, just after the nuclear power accident in Chornobyl. The now classical book is divided into three parts addressing the contours of the risk society, individualisation, and reflexive modernisation. The theoretical perspective addressed and applied in this dissertation is mainly rooted in Beck's, and to some extent, the British sociologist Anthony Giddens' seminal work on risks in the risk society. Their works on risk and the risk society, which was mainly conducted independently, gained the attention of a wide audience, and has since been developed further, and grown into a large body of literature.

For a brief introduction to the risk society thesis, the logic of societal 'goods' and *manufactured* 'bads', will be related to one of the myths about King Midas.

> *King Midas is offered a wish from the god Bacchus in return for a good deed, and King Midas wishes that whatever he touches may turn to gold. The wish is granted, and Midas possess the ability to transform anything into gold. However, the 'golden touch' works without exemption and Midas discovers*

> *he cannot even eat or drink. His gift for eternal wealth will also be his death sentence. Midas begs Bacchus to relieve him from the 'golden touch'. His wish is once again granted, and Midas is freed from his fortune and curse.* (Ovid, 2018: 261-263)

In simple terms, the myth illustrates how the quest for wealth may be accompanied by unintended side effects. In the risk society, technological advancement is our 'golden touch'. However, society's successful technological advancement is accompanied by new risks, which can threaten human life itself (Beck, 2006: 329). Giddens (1998: 27-28; 2002: 26) defines the new risks as *manufactured* as opposed to *external*. The 'old' and external risks are experienced as originating from outside ourselves, such as natural events. Manufactured risks are however created by humanity's knowledge and impact on the world, such as nuclear risk (Beck, 1986: 8) and cyberrisk (van Loon, 2000, 2002; Lupton, 2016).

In risk studies, risks are typically defined in relation to their consequences (Society for Risk Analysis, 2018: 4). In the risk society however, manufactured risks are defined with respect to their cause and their creator – us. Ironically, the scientific and technological progress meant to solve problems, has created new risks (Arnoldi, 2009: 46). Therefore, risk becomes the all-consuming focal point in the risk society.

> *"How extraordinary! The riches, longest-lived, best-protected, most resourceful civilization, with the highest insight into its own technology, is on its way to becoming the most frightened."* (Wildavsky, 1979: 32)

As Giddens (2002: 26) explains this transformation, Western societies at a certain point "started worrying less about what nature can do to us, and more about what we have done to nature". This paradoxical and problematic relationship between perception, technological advances and risk, has been a topic of interest for researchers for decades (Caygill, 2000; Douglas & Wildavsky, 1983). For example, why asbestos poisoning, a potential side effect of a product developed to save people from burning, is perceived

as more frightening than fire (Douglas & Wildavsky, 1982: 50). We live in a state of vague, low-level fear (Massumi, 1993: 24) because everything might have the potential for a crisis. Everything constitutes a risk, and therefore, risk consumes us. This is particularly true for global risks, which have a broad reach and are intangible.

2.2 Intangibility of global risks

Within global manufactured risks lies the dilemma, which is that we struggle to, or cannot foresee the risks ahead of time. Compared to traditional risks, like industrial accidents, wars and earthquakes, global manufactured risks tend to be intangible, latent, and not immediately noticeable (Arnoldi, 2009: 47; Beck, 2009: 19). This leaves society in a position of limited knowledge about what the future may hold and how to manage it.

> *"A risk society is a society where we increasingly live on a high technological frontier which absolutely no one completely understands and which generates a diversity of possible futures"* (Giddens, 1998: 25)

The perception of global risks is distinguished from earlier risks with the three features of *de-localisation*, *incalculability*, and *non-compensability* (Beck, 2009a: 52-54).

De-localisation

Beck (2009a: 52) divides the de-localisation of global risks into three levels: *spatial*, *temporal*, and *social*. Spatial refers to borders, temporal to latency, and social to the complex and unforeseeable ripple effects. One of the key characteristics of global risks is that its impacts are not immediately visible and is not limited to a certain geographical area. In contrast to smog and deforestation, which are examples of local risks, the influence of global warming, a de-localised risk, has latency and is a slow change. The consequences might manifest themselves to future generations. For instance, in the 1970s, some scientists discussed whether the world was experiencing global cooling (Giddens, 2002: 29). Within this lies the dilemma that ripple effects of

humanity's activity, such as extreme weather, cannot be interpreted as the cause and consequence of a phenomenon with absolute certainty.

Global risks are de-localised, and in principle, omnipresent (Beck, 2006: 333). They tend to be independent of national borders, social class, established institutions and even principles of time. Additionally, the cyber domain requires us to rethink what is 'local' as a result of globalisation, networks and communication technologies (van Loon, 2000: 168-169). Consequently, cyberrisk is particularly challenging to 'localise', conceptualise, interpret, and to understand.

Incalculability

The principle of calculation is a key difference between risks in the risk society and more traditional understandings of risk within risk studies and economics. The risk society thesis is concerned with incalculable risks. The traditional tools of assessment and management, which are typically based on historical data and projection, are no longer effective. In other words, the established calculation by science and legal institutions "collapses" (Beck, 1992b: 22). A retrospective approach might even encourage anticipation of the 'wrong' risks (Beck, 2006: 330), meaning that the past is likely to be a poor indicator of the future where we might face unknown unknowns or 'black swans'. Hence, the intangibility of global risks is not only a challenge to laypeople, but also to professionals trying to calculate risk.

In risk studies and economics, uncertainty is traditionally defined as unmeasurable, whereas risks are understood as the opposite, measurable through calculations or statistics (Knight, 1921: 233). Beck later attributed the dissonance between the terms risk and uncertainty in risk studies and the risk society, to the fact that he was not familiar with the terminology and definitions in use (Sørensen, 2002: 125). However, it can be argued that this has been a fruitful 'mistake' as it has led to further explanations, definitions, and explorations of the risk concept (Sørensen, 2018: 7), including in Beck's own work (see e.g. Beck, 2009b: 295-297). Theoretically speaking,

risk always contains an element of uncertainty (Mythen, 2004: 14), as risk reflects what might happen (Adam & van Loon, 2000: 2), and not a certain outcome. However, because the risk literature no longer has a clear distinction between the two concepts (Pettersen, 2016: 40), and the term risk is more often applied in the cyberdomain, this dissertation will continue to use the term risk.

Non-compensability

Challenges to calculating risk are also reflected in the challenges to compensating risk, which is typically operationalised as insurability. Events that occur regularly (in a population) become broadly calculable, and in that sense also insurable by both private insurance and the welfare state (Giddens, 1999: 4). Risk and insurance are historically interlinked from the early use of the term 'risk' in seafaring, where risks were estimated to the extent possible, and maritime insurance was issued accordingly (Ewald, 1993: 226). When Beck addresses manufactured global risks, he referees to them as uninsurable. The global manufactured risks, such as cyberrisk, terror attacks and climate change, have a different scale and aptitude than what can traditionally be calculated in a population. However, empirical data have contested insurability. For instance, while acknowledging how insurance capacity is threatened by long-tailed and event-specific risks, Ericson and Doyle (2004: 168) showed that insurance was applied after the 9/11 terrorist attack even though the risk could not be calculated.

While insurance is one aspect of compensation, another aspect is the irreversibility of risks. Ewald (1993: 222-223) argues that the new generation of risks cannot be insured. This is because ecological risks caused by human activity and technological processes, have the potential to affect life itself and its reproduction. In these cases, given the unrepairable nature of damage, the effects are not only incalculable but also non-compensable. Their severity thus, represents a shock for humanity (Beck, 2006: 330).

The three features of intangibility can be summarised with the example of the nuclear power accident in Chornobyl. This accident was later attributed to a flawed reactor

design and inadequately trained personnel (World Nuclear Association, 2022). The damage from this explosion has had and will have a lasting impact on people's health and the environment. Although the area and people around the reactor were the most heavily affected, it is challenging to conclude which effects should be attributed directly to the accident. The effects were, and to a degree, are still incalculable. The effects we know of and which we can calculate, are broadly de-localised in time and space. For instance, 35 years later, levels of radioactivity in a sample of grazing animals in certain areas of Norway, is still being controlled for food safety (Norwegian Food Safety Authority, 2022). Furthermore, the magnitude of the effects and the challenges in calculating them, are reflected in the limited possibilities of providing compensation. The three are clearly linked, as de-localisation is a challenge for calculation which consequently challenges the possibility to compensate.

2.3 Intangible risks as a managerial problem

Scholars of both sociology and management accounting, emphasise how more and more aspects of life are described in terms of risk (Lupton, 2013: 3; Power, 2007: 1). The intangibility of risks intensifies the challenges for management. While intangibility is a conceptual problem in the risk society, it is a managerial problem in management accounting and for practitioners. The implication of manufactured risks is that we have limited knowledge and experience in how to manage them (Giddens, 2002: 26). The latent and borderless character of global risks limits the ability of organisations to identify them, raising the dilemma of *whose* responsibility the consequences are. For management purposes, uncertainties should be translated into risks (Themsen & Skærbæk, 2018), to at least allow for the *intention* of management. Furthermore, incalculability is a challenge for documenting results and for legitimising control. After all, managers depend on the 'visible' management of risk to document 'visible' results. Risks therefore should be auditable (Power, 2004: 10). Lastly, when risks are non-compensable in terms of them being uninsurable, organisations lack a 'security net' if there is an accident or crisis.

The risk society, later addressed as a *world* risk society (Beck, 2009a), is concerned with intangible global risks, which call for global solutions. Besides discussing overarching solutions for politics and regulations, sociology is limited in addressing how risk can be managed on an organisational level. Nevertheless, managers are expected to manage the impacts of global risks at the organisational level. The concept of risk implies an 'object of management', which implies responsibility as part of an organisation's legitimisation (Power, 2007: 6). Managers are hence trapped in the dilemma of not knowing the risks they face, but must act *as if* they do (Douglas & Wildavsky, 1982: 49). Risk is increasingly seen as something that can be managed and therefore associated with responsibility and blame (Lupton, 2013: 37). Intangible risk means seeking answers to questions that no one can formulate clearly (Beck, 2009a: 115). As a result, the ambivalence in assessing risk tends to paralyse action (Lupton, 2013: 83).

The risk society thesis places *unmanageable* risks which pose a danger to society, at the forefront (Mythen, 2021: 535). Regardless of whether the risk is considered manageable or not, the standard response to crises and accidents of both small and large scale in the Western world seem to be: 'was the risk assessment (in)sufficient? Was the routine followed?'. The expectation for managing global risks at a local level is problematic for authorities and organisations tasked with managing risks. Living in a risk society means facing the "awkward problem" of having to sometimes make crucial decisions based on limited knowledge, or non-knowledge (Beck, 2006: 335). This raises several managerial dilemmas, such as: 'how do you interpret global risks that are intangible per se? How do you manage global cyberrisk at a local level well knowing that global solutions are called for? Which interventions are enough when nothing is enough? How do you make decisions and manage the unmanageable?'.

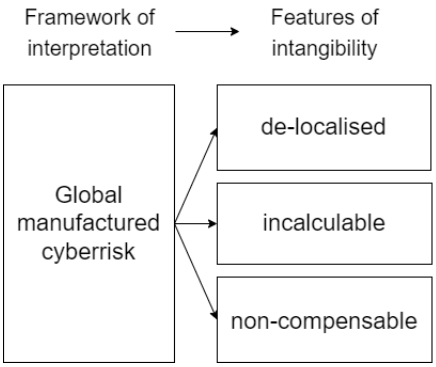


Figure 1 Overview of theoretical framework

As summarised in Figure 1, the suggested framework for global manufactured risks implies that cyberrisk is intangible, as it is *de-localised*, *incalculable*, and *non-compensable*. Due to increasing digitalisation and cyberattacks, cyberrisk is a concern for management, because it is challenging given that its risks are intangible. Subsequently, the question of how managers may interpret and intervene with intangible cyberrisk, is explored in this dissertation.

3 METHODOLOGY

To study the complexity of how intangible cyberrisk is interpreted by organisations, a methodology allowing for rich explanations and adaptions to the project during its course is required. The methodology chapter starts by addressing the motivation of the PhD project, and more importantly how interaction with the industry and 'discoveries' along the research process led to the development of new research questions. Section 3.2 addresses the philosophical stance of the dissertation. Furthermore, the methods used to gather and analyse data for the articles in the dissertation are elaborated on in section 3.3. Finally, section 3.4 presents a reflection on the role of an industrial researcher.

3.1 Journey of discoveries

The methodology in this PhD project can be described as an interactive journey, which is arguably a useful approach to qualitative research, as allows the researcher to follow 'discoveries' along the process, and prompts the formulation of 'appropriate' research questions (Agee, 2009: 432, Willig, 2013: 27).

As this is an industrial PhD project, it started with a practical problem and concern. This project started in an IT company working closely with the Norwegian power industry, typically on IT projects and operations where additional resources and competence within network and security are needed. Over the years, security challenges became more prominent (and security services more in demand). I learned that there were several reasons for this. For decades, control switches operating generation, transmission and distribution of power had been manually operated and therefore 'spared' from cyberrisk. In recent years, however, the situation had changed due to increased digitalisation, such as centralised operations and troubleshooting, automation, use of cloud services and the smart meter. Larger modernisations of the industry had introduced new security challenges both to operational technology (OT) and information technology (IT) – and perhaps especially in the intersection between

the two. On the OT side, operations had to adapt to new technology and increased vulnerability. On the IT side, we observed a growing number of fraud and small-scale attacks, typically emails aiming to socially manipulate the recipient to transfer money. Parallel to digitalisation, the industry's preparedness regulations were in the process of an update with particular attention to cybersecurity. All in all, security was no longer only a part of 'good IT practice' but a defined field; hence, my initial question was: how are cybersecurity risks managed in the Norwegian power industry[1]?

The initial research question led me to risk management literature and previous studies of cyberrisk and its counterpart cybersecurity in electricity distribution companies. As a 'pilot study' to learn more about the context, I began by engaging in dialogues with the industry, authorities, colleagues, and my network within cybersecurity, as well as looking into reports and data by authorities and security companies. I conducted interviews and asked questions like "how do you define an incident?" and "which incidents affect your organisation?". Previous research had found that the industry had challenges providing a clear definition of an incident (Line et al., 2016: 18). However, I found that the actors in the industry, from personnel to security companies and even authorities within Norway have widely different definitions of what an incident is. I learned that the word 'incident' could be interpreted on a scale from 'something is happening' including either good or bad, to 'critical events to operations'. To exemplify, 'an incident' could mean a spam email that was automatically blocked by the spam filter to some organisations and damaging malware infections to others. I also asked more open questions to learn about their perceptions of risk. I asked questions like: "what would the worst case scenario be?",

[1] My focus was on electricity distribution companies, i.e. the 'last mile' in the power supply chain. Each electricity distribution company has a geographical monopoly and an obligation to distribute electric power to households, companies, industries, and public buildings in their area. As the energy production in Norway is based on several highly reliant hydropower stations, the distribution, rather than the production, is seen as the most critical actor in the supply chain. For simplification purposes, the term 'power industry' or 'industry' is used in this dissertation when referring to electricity distribution companies.

"what do you consider the most likely scenario?", "which challenge within cybersecurity worries you the most?" and "what do you consider most important to reduce cyberrisk?" Once again, the responses I got highlighted a broad and divergent spectrum of cyberrisk and 'trends'. From 'not-so-worrisome' spam emails, to a deep-felt concern for how fake news may cause substantial harm on a societal level. I discovered that although 'everyone' emphasised the importance of cyberrisk, and that there is a challenge or problem, there was a challenge to define what the problem within cyberrisk is. An incident could mean 'anything' and the industry's understanding of cyberrisk was less solid than I had hoped for – it was more like gas.

Scouting academic literature for research on cyberrisk and how it is defined, has been an ongoing process to guide my research. I knew that cybersecurity was considered broader than related fields of information and ICT because it also considers the human element and society at large (von Solms & van Niekerk, 2013: 100-101). These are in fact some of the reasons why the term cyber is recommended to replace similar terms when possible (NSM, 2015; 40; Ramirez & Choucri, 2016: 2232). I was therefore somewhat 'disappointed' to discover that the "canon" (Strupczewski, 2021) of defining cyberrisk was limited to information security (Cebula & Young, 2010: 16), which is arguably too narrow. Moreover, a surprisingly large number of formal definitions of cyberrisk overlooked defining 'risk', which can result in very different understandings. As research on cyberrisk is interdisciplinary and relatively new, academic literature admits that the lack of common terminology is a research barrier (Falco et al, 2019; Ramirez & Choucri, 2016), and less of a fruitful academic discussion.

At this point, I was (at least) one problem richer than when I started the project. This was a problem of what cyberrisk is, not only a problem of how to manage the new cyberrisk. One important event for the industry at the time, was the updated version of the preparedness regulations with major revisions concerning cybersecurity. This gave me an opportunity to study how cyberrisk and regulations are perceived and translated into internal routines. I found that cyberrisk is perceived as complex and

challenging by the industry. The regulations instruct the industry to assess and mitigate cyberrisk, but gave limited guidelines concerning acceptable risk, how it could be mitigated, and more importantly: what the risk was. The industry had a reputation for being skilled in managing situations concerning physical disturbances and incidents. However, managing cyberrisk was seen as a less mature field. A common explanation was a lack of experience in managing targeted cyberattacks (Line et al., 2016: 24; Hagen et al., 2017: 30).

In addition to the recurring question of what risk *is*, I had picked up on an ongoing 'debate' in my pilot study concerning information sharing. Some actors remarked that the information sharing from the authorities and non-governmental organisations seemed rather 'asymmetrical' and 'organisation-dependent'. While some were interpreted as quite open, others had the reputation of being more restrictive. A restrictive practice could be justified in security concerns, although competing explanations were present. To simplify, the question was: Is there important information about cyberrisk which is not shared?

My pilot study had identified several risk reports and threat assessments. To *identify* the risks, I wanted to summarise 'overall cyberthreat'. On one hand, the work led to the identification of the 14 most dominant cyberthreats in the reports. But on the other hand, I also found that the descriptions of risk provided were sometimes vague and conflicting. Additionally, I was 'haunted' by the fact that cyberrisk is evolving, which implies that the identified risks are also likely to change. The industry cannot wait for authorities or academia to define or 'benchmark' risk. I was convinced that cyberrisk was still worth at least trying to understand, but different approaches were needed. This became a turning point for me as a researcher, and I subsequently decided to distance myself from the empirical context where my research had begun to be able to see the bigger picture of how we can gain knowledge, interpret and understand unknown cyberrisk.

The 'debate' on information sharing and the lack thereof identified in the threat reports, suggested a large potential for knowledge sharing and knowledge generation. I used theory of risk and communication to demonstrate this potential. A further approach to understanding unknown cyberrisk was motivated by the potential of unknown futures. This led to a conceptual discussion based on literature on risk management, and scenario analysis in relation to cyberrisk. Finally, the last approach was motivated by my fascination with economic crime and study how an organisation can gain knowledge about seemingly 'cryptic' ransomware attacks through theory of business models.

As Marcel Proust (1929/2014: 236) characterised "the only real voyage of discovery", it is not to seek strange lands or landscapes, but to possess other *eyes*. While my search for new landscapes can be described as a turning point, my search for new eyes was more of an ongoing concern.

During the research process, the theoretical frame of risk management was reconsidered on several occasions and discussed with my supervisors. Although the literature is broad and to some extent adapted to manage complex cyberrisk, I was reluctant to 'fit' cyberrisk into the risk management frame. One of the reasons was that risk management is criticised for becoming a legitimisation process rather than managing risks (Power, 2009: 854). Another concern was lack of consistent benefits from enterprise risk management systems, and on the contrary, the documented harm to the most eager users, such as banks during the financial crisis (Bromiley, 2015: 273). Based on my experience in the industry, risk management frameworks were seemingly either too extensive for practice and/or led to gross simplifications of cyberrisk (e.g. red, yellow or green). For instance, the recommended framework for IT security for the industry at the time consisted of 142 recommended measures. Even though enterprise risk management has been adapted to include cyberrisk, the success to do so has been questioned (Eling et al., 2021; Marotta & McShane, 2018), and the

risk assessment is arguably unlikely to identify, and therefore manage, novel cyberrisk and 'black swans' (Refsdal et al., 2015: 123-124).

Since cyberrisk as a field is considered relatively new and dominated by technical research, the existing body of literature offered limited guidance on how organisations interpret and manage cyberrisk. In addition to the technological perspective, several scholars study cyberrisk from an insurance perspective. However, my reason for not pursuing this body of literature further was not only academic. My moral compass did not align with the 'solution' this body of literature offered, as the literature identified largely neglected fundamental ethical considerations such as whether cyber insurance contributes to maintaining and facilitating cybercrime.

After moving back and forth between theory, data and the concept of cyberrisk, and having discussions with my supervisors, I found the risk society thesis helpful for interpreting cyberrisk. The risk society thesis offers a theoretical framework to explain the two facets of cyberrisk, as both technological advancements and unintended side effects, and also offered a framework for investigating intangibility utilised in the dissertation.

These 'discoveries' led me to realise that managing cyberrisk is not hard because it is new, instead, it is hard because the risks are intangible, and that waiting for them to 'stop being new' is not an option. The important question was therefore not how to adapt an enterprise's risk management system to cyber, rather the question was how to understand risk. As a result, we need to explore how to define, think about, and prepare for risks we do not know how, where and when will occur. How can we prepare for cyberrisk we do not really grasp? How can we handle intangibility? All four articles address challenges of intangibility of cyberrisk and explore paths to increase tangibility, to understand and interpret cyberrisk. The dissertation goes more in-depth and unifies the four articles by adding the theoretical lens of intangibility of global manufactured risks in the risk society.

3.2 Philosophical stance

The ontology and epistemology of risk has been subject to academic debate (Rosa, 1998), in particular, whether risk is *objectively given* or *socially constructed* (Hansson, 2009). The dominant view in risk analysis is that risk can be characterised in terms of objective facts about the physical world, such as probabilities (Hansson, 2010: 232). Risk as objectively given seems to hold the longest tradition, and one of the oldest formal definitions is risk as expected loss, attributed to De Moivre in 1711 (Aven, 2014: 22-23). A main critique of objective risk measures is that they do not account for values and the social, political and cultural contexts (Rosa, 1998: 19-21). Although risk as an objective measure (e.g. a probability function) is argued to be too narrow by some, it is still applied (and found suitable) in other contexts (Aven, 2014: 27-30), e.g. insurance and medicine.

Jasanoff (1999: 150) argues that social science has altered our understanding of risk from *real and physical* to *constructed and relative*, where meanings vary between social groups. In the social sciences, risk is often seen as a social construct. 'Strong' constructivism is found in the works of Mary Douglas and colleagues (Douglas & Wildawsky, 1983), where they argue that risks are culturally biased, collective constructs influenced by both public perception and social organisation. Therefore, the aspects which are seen as more or less worrisome can vary across cultures (Dougolas & Wildawsky, 1983: 186). Strong social constructionism implies that risk does not (necessarily) refer to any objective facts about the world (Hansson, 2010: 233).

Beck can be described as reluctant to position his research within an epistemological tradition. In his own words, epistemology was a "pragmatic" concern based on the questions studied (Beck, 2000: 211). However, the works of Beck and Giddens on risk are commonly classified as weak constructivism or constructivist realism (Strydom, 2002: 46-52). This constructivist understanding of risk does not reject that risk has an *objective core* (as opposed to strong constructionism). Although the risk has an objective

core, they become risks in our perceptions of them. Additionally, our understanding of risk contributes to reproducing and changing risk (Sørensen, 2018: 8).

This dissertation follows a weak social constructivist position where the concept of risk is socially constructed around an objective truth, infused with meaning through our understanding of the world. This epistemological position opens for studying how risk is understood, rather than objectively measured (positivism) or pure perception (strong constructivism). While strong constructivism can be seen as undermining human intervention (Lupton, 2013: 42), this dissertation is based on the assumption that risks are influenced by human understanding and action, and therefore humans have the power to influence risk. This position is applied as a frame to study how risk gains importance and attention, and how risk is interpreted as well as understood.

3.3 Methods: Qualitative data collection and analysis

To be able to explore the intangibility of cyberrisk, this dissertation applies a *qualitative* research approach. The variations in methods within qualitative research is a consequence of aiming to explore and understand the multifaceted phenomena of cyberrisk. The type of article, method, sample, data and analysis are summarised in Table 1 below. The table also summarises how the method contributed to defining the problem and exploring different perspectives to make cyberrisk more tangible, as described in section 3.1.

	Article 1: **Regulations**	Article 2: **Openness**	Article 3: **Foresight**	Article 4: **Strategy**
Type of article	Research article	Research article	Conceptual article	Research article
Method	Case study	Content analysis	Conceptual discussion	Content analysis
Sample	1 'unique' case	7 reports	Articles	4 attack cases
Data material	**Observation:** **1** seminar about new regulations **Participant observations:** **2** preparedness exercises **15** project meetings **Interviews:** **8** semi-structured interviews **Document:** Public hearing, reports and announcements	**Documents:** **7** risk assessments and threat reports	**Literature:** Risk management; Foresight; Scenario analysis	**Online sources:** News articles; Blogs/magazines; Webpages; Press releases
Analysis	'Empirically close' coding + grouping	Content analysis: Cyberthreats/risks Openness	Conceptual analysis	Deductive content analysis: Business model canvas
Contributed to	Define the cyberrisk problem	Define baseline and explore cyberrisk through openness	Explore cyberrisk through foresight	Explore cyberrisk through strategy

Table 1 Overview of methods

To present the methods as clearly as possible, the following sections are organised in the subsequent order of the four articles.

Methods for studying cyberrisk and regulations (article 1)

Studying how cyberrisk regulations were perceived and translated into internal routines, took form as a case study. One project group (case) was followed throughout a project organised by their industry association with the aim to 'operationalise' the updated preparedness regulations concerning cybersecurity into internal routines. The material the project group produced was then distributed to the other companies in the industry association. The project group consisted of a project manager from the

industry association, representatives from six different electricity distribution companies, and an external consultant. The consultant had the opportunity to include more consultants if requested by the project manager. The participating power companies were small or medium-sized, used different internal control systems and routines, and were located in different parts of Norway. The data gathered consisted of observations, interviews and documents.

Prior to the commencement of the project group, **observations** took place during an informational meeting about the changes in the regulations. The meeting summarised the reactions to a public hearing about the new regulations, and the authority's considerations and responses. The observations offered an important introduction to the process and showed 'tensions' between the industry and the authorities. In addition, observations (as participant) were conducted during two preparedness exercises with 20 participating power companies. The preparedness exercises were conducted as tabletop exercises with pre-developed scenarios and questions to facilitate discussions. The discussions of different scenarios, from fire to cyberattacks, informed my preunderstanding of preparedness towards different kinds of incidents.

In the project group, I took the approach of **participant-as-observer**, which means my role and intentions as a researcher were openly communicated while participating (Easterby-Smith et al., 2018: 211). Participant-as-observer can be helpful in gathering rich data and examining research questions that emerge throughout the process (Jorgensen, 2015: 1-8). I was invited to project meetings and also included in the project's shared digital workplace and general email correspondence. I followed the project closely from the beginning to the end which included, its kick-off meeting (two days), ten status meetings (30-120 minutes each), a seminar (one day), a workshop (two hours), and its concluding meeting. The kick-off meeting and the seminar were physical meetings. The workshop and all status meetings, including the concluding meeting, were held using a conference tool. Notes were taken during all workshops, the seminar, and the meetings. I made a thick margin on each page in my notebook to

separate field notes from the actual discussions, views, and actions in the meeting on one side from my own thoughts, interpretations or follow-up questions on the other side. Tape or video recordings were not used during workshops, the seminar or meetings, as this could have been experienced as 'intrusive'. However, the participation and close cooperation with group members provided good opportunities to 'revisit the data' by asking follow-up questions and discussing different matters more thoroughly.

The **interview data** consists of formal interviews with the project manager, four participants and three external consultants. Interviews were recorded, which allowed for greater focus on the conversations taking place and helped me avoid 'jumping to conclusions' just from my notes. Most of the interviews were conducted shortly after the concluding meeting to allow for time to build trust between the interviewees and me as a researcher, and to let the observations guide the interviews. The interviews were semi-structured using two to three topics for conversation, which were communicated to the interviewee in advance. Small variation in topics reflected the person's role in the project, e.g. project manager or consultant. Prior to the interview, a list with sub-questions for each topic was prepared. Sub-questions were not distributed to the interviewees, but used as 'conversation starters' or asked if they were not naturally covered by the conversation. In this sense, the interviews were *prepared*, rather than structured. Variation in prepared sub-questions reflected the person's involvement in the project, as some participated actively throughout the whole project period, while others were active only in parts of the project. The interviews were conducted either face-to-face, or using a conference tool/telephone, and each interview lasted on average around 45 minutes. Follow-up conversations were conducted with two interviewees for more detailed information.

In addition to **documents**, i.e. field notes, generated through observations, an important secondary source of data was a report based on the public hearing of the

proposed changes in the regulations. This report included comments based on statements from 40 independent actors, as well as comments from the authorities.

The data **analysis** was conducted in phases. The first phase took place during the months in which the project group worked together, and the second phase took place after this period. Field notes taken during observations were processed after meetings. Since the translation process was of interest, I extracted the group's methods, activities, and steps from my field notes. Moreover, I extracted data that could enlighten risk perception, risk appetite, and attitude towards risk regulations. As the document analysis and observations were mainly conducted prior to the interviews, they were used to inform the interview guide. The second phase of data analysis was the coding of interviews to 'capture the essence' in shorter keywords or phrases. As the interviews were recorded and transcribed, it allowed for a more thorough analysis than the analysis based on my field notes. The interviews were also an opportunity to 'distance' myself from the role of a researcher-as-participant and to let the interviewees talk freely without being influenced by the group. I started the coding process by 'getting to know the data' which was done by listening to the recordings several times. I then developed 'empirically close' codes from the transcriptions. More specifically, this means that the first set of codes are derived from the data, and the procedure is intended to reduce the chance of jumping to conclusions based on 'gut feeling' (Tjora, 2019: 28-29). The codes generated were typically short passages of text, either as a direct quote or as a summary. This allowed for more of the context and meaning to be kept in the codes and to avoid 'premature' simplifications. The codes were then grouped into the categories of 'risk perception and risk acceptance', 'guidance', and 'rules as legitimacy'. The coding of interview data was used as the final analysis, and the main findings are presented in article 1 in this dissertation.

As described in the first article, the industry perceived cyberrisk as complex and challenging, and indicated that they lacked guidance in terms of what would be considered 'sufficient' security or risk management. The study showed that, what the

risk is, could be unclear and that increased information sharing was requested by the industry. The subsequent data analysis and research questions are based on the finding of these issues.

Methods for studying cyberthreats and openness (article 2)

As the industry experienced difficulties defining which of the risks to emphasise based on the regulations and translation process, I wanted to investigate the available information about cyberrisk and aimed to summarise 'overall cyberthreat'. Furthermore, both pilot study and study of cyberrisk and regulations had revealed some 'debates' concerning information sharing from the authorities. I therefore wanted to study how information about cyberrisk was communicated and shared, and the potential of openness to explore risk.

The data gathered and analysed in this process consisted of **documents**, more specifically risk assessments and threat reports. The reports selected were openly available and considered relevant for Norwegian companies. In addition, as cyberrisk is characterised by fast change, reports older than two years were not considered. Lastly, reports by public authorities and non-governmental organisations were preferred. Based on these considerations, I selected seven reports for further analysis. Four reports were published yearly by the Norwegian authorities. These were supplemented with three reports with special attention to cybersecurity and cybercrime. An overview of the analysed reports is presented in article 2.

The reports were analysed based on **qualitative content analysis**. Content analysis is about drawing inferences about the phenomena researched (Krippendorff, 1989: 407). Typically, the goal is to "reduce the material" (Flick, 2009: 323), which in my case meant to compose a comprehensive overview of cyberthreats. The reports were analysed with attention to two aspects: (1) cyberthreats/risks, and (2) openness. As for the second aspect, I looked for content concerning information sharing and advices or suggested measures in the reports. The identification of cyberthreats was (more)

straight-forward. Cyberthreats were coded as single words or terms when possible, but more often as short passages of text. I also took note of the report and the page numbers to easily revisit the code if necessary. Each specific cyberthreat was only 'counted' once in each report, e.g. if 'ransomware' was mentioned several times in the same report, it was counted one time. Similar to the approach of 'empirically close' coding, short passages of text from the reports were gathered to avoid misplacing codes in the categorisation phase due to lack of context. However, this also meant that many individual codes were produced. This process left me with 177 codes of cyberthreats in an Excel sheet. The table below shows an example of the codes for cyberthreats generated.

Cyberthreats	Report	Page
Open access malware and outdated vulnerable systems	NSM	11
Jamming	E-tjenesten	8, 27
Fake message of changed bank details	NorSIS	13
Data breach by foreign states with purpose of espionage and intelligence gathering	Mørketallsundersøkelsen	44
Ransomware and cryptoware	DSB	198

Table 2 Example of codes generated of cyberthreats

The next step in the content analysis was the categorisation of the codes. The work was done manually by first categorising identical codes, then checking for strong similarities between categories and grouping those together. As I aimed to identify the dominating cyberthreats, only cyberthreats addressed in more than half of the reports were considered further. The remaining codes were rejected. Lastly, a colleague specialised in cyberrisk looked through the categorisation of codes to validate the process. The analysis resulted in 14 cyberthreats. The cyberthreats and examples of each category are presented in article 2. As indicated, extracting content based on openness was more complex. The reports were analysed to identify suggested measures, content about information sharing, e.g. reporting, and how threats and risks were communicated. Furthermore, the 'evaluation' of openness was influenced by the number of threats and measures shared. The results were therefore presented in a descriptive text.

While article 2 presents 'overall cyberthreats', it also confirms that cyberrisk can be challenging to understand. Moreover, the possible gains and challenges related to information sharing are elaborated. Hence, a related question is how unknown unknowns can be explored by the organisation.

Methods for studying cyberrisk and scenario analysis (article 3)

Studying how foresight and scenario analysis can be used to gain knowledge of unknown cyberrisk took the form of a conceptual analysis. The method can be used to analyse existing literature to explore a concept, theory, subject, or field. This analysis was based on articles from the field of risk management and scenario analysis and foresight, and then related to the field of cyberrisk. The sampling of articles from the substantial bodies of literature used in the analysis was based on the main author's academic experience in the fields of risk management and scenario analysis.

The first step was the analysis of risk management literature to identify and 'problematise' the main critique or weaknesses. In particular, the literature was analysed with regards to how the weaknesses may constitute serious limitations for managing cyberrisk. The analysis identified two main critiques of traditional risk management. The first is that traditional risk management creates an 'illusion of control' where risks are underestimated and the ability to manage risks is overestimated. The second is that traditional risk management based on historical data is inefficient towards 'black swans', such as novel cyberattacks. The next step was the analysis of literature within foresight and scenario analysis with regard to two aspects. First, how scenario analysis may 'fill the gaps' of traditional risk management, and second, a critical review of potential dilemmas and pitfalls.

Articles 1 and 2 have shown that cyberrisk is perceived as complex and challenging to understand, while articles 2 and 3 have addressed cyberthreats and unknown unknowns. To apply knowledge about cyberthreats in a useful way, a related question is how they can become easier to communicate, interpret and understand.

Methods for studying cybercriminal's strategies (article 4)

Studying cybercriminal's strategies was based on four attack cases. The cases were selected purposely based on variation and available information. First, the four cases were believed to illustrate key variations in how ransomware attacks are conducted. The choice to interpret these variations as different business models introduced the possibility of understanding ransomware based on an existing well-defined business model (Osterwalder & Pigneur, 2010). Second, a decisive factor was the available information to minimise "serious data limitations" reported in most research on cybercrime (Maimon and Louderback, 2019: 208). The selection of cases was discussed with cybersecurity professionals to test whether the sampled cases were perceived as providing insights into variation. The broad search in the data collection phase, and the snowballing effect of addressing attacks in the media sources, allowed for several cases to be considered representative cases regarding variation, whilst offering the necessary information. Similar cases were identified, but as the intention was to illustrate variation, the four cases were seen as sufficient.

Based on ethical and practical considerations, the data material consisted of **text-based online sources**. The internet undoubtedly provides a wide range of easily accessible data, but this is not without its limitations and must be assessed critically. Data were evaluated based on the criteria content, source and author. The content had to describe a relevant ransomware attack or criminal group. The source must have been of relevance to the general public and/or the cybersecurity community. The author or editor (person or institution), must have been named. In addition, multiple sources were used to describe each case. These sources included news articles, IT/cybersecurity-specific magazines/news/blogs, content from security companies, and press releases from targeted organisations. An advantage of using documents is that the data is produced without the researcher's intervention and is therefore "naturally occurring" (Silverman, 2014: 276). Another advantage is that the research design also allows others to examine the sources and reproduce the results as they are

publicly available. Data were identified through: 1) tips from cybersecurity professionals; 2) searches on Google, IT/cybersecurity-specific news sites and content from targeted organisations; and 3) snowballing, e.g., following cross-references in the data to other data sources and cases.

Content analysis is widely used to analyse text, particularly for material from the mass media (Mayring, 2019). The content analysis followed a structured, deductive approach. In a deductive approach, a categorisation matrix is developed, and data is coded according to the categories (Elo & Kyngäs, 2008). The categories, or themes, and corresponding descriptions and examples in this study followed the building blocks in the business model canvas (Osterwalder & Pigneur, 2010). The analysis was structured in that only data that fit in the categorisation matrix was chosen and subject to further analysis. This categorisation matrix is presented in Table 3 below.

Category (building block)	Description	Examples
Customer segments	One or several group(s) from whom the company creates value	Mass market, niche, segmented, diversified, multi-sided
Value proposition	Product and/or service offered to the customer segment	Customisation, "getting the job done", price, cost reduction, risk reduction, accessibility, convenience
Channels	Communication, distribution, and sales channels to reach the customer	"Channel phases": awareness, evaluation, purchase, delivery, after-sales
Customer relationship	Type of relationship established with (each) customer segment	Personal assistance, self-service, automated services, co-creation
Revenue streams	Cash generated. Transaction revenue (one-time) or recurring revenue (ongoing)	Asset sale, licencing, brokerage fees, etc. Pricing mechanisms: fixed or dynamic
Key resources	Most important assets	Physical, intellectual, human, financial
Key activities	Most important actions	Production, problem solving, platform/network
Key partners	Critical network of suppliers and partners	Strategic alliance, coopetition, joint venture, buyer-supplier
Cost structure	Incurred costs while operating the business model (cost-driven or value-driven)	Fixed costs, variable costs, economies of scale, economies of scope

Table 3 Categorisation matrix

Data about the selected cases were gathered and analysed seeking information concerning the nine categories in Table 3. Some categories were more challenging to find reliable, or any information about. 'Key partners' in particular, could only be identified, at least to some extent, in two cases. Data were gathered until saturation was reached, meaning that additional data did not add to the business models.

3.4 The role of an industrial researcher and research ethics

As an industrial researcher I found myself very much in the data, almost to an extent where I am the data. The advice "don't rush to the data" seemed out of context. Instead, I dove in. I engaged in dialogues with the industry, authorities, industry associations, partners, colleagues, and my personal network. I prioritised attending numerous industry conferences, invited, visited, and scheduled meetings with authorities and stakeholders in the industry, as well as participated in preparedness exercises and research seminars. I observed, listened, and talked to stakeholders in the Norwegian power industry, and I learned from the formal events, such as conference talks and interviews, as well as conversations in breaks and over dinners. Through my employment, metaphorically and literally speaking, I got a place at the table.

This illustrates one of the important advantages I had as an industrial researcher: building on the network of the company, and over time, my own network, was fruitful for getting in contact with people, scheduling meetings and discussing cyberrisk. Having someone to vouch for me earned me their time. For instance, my experience of reaching out to other companies in other industries where neither I nor my company had a relation with, was not very successful. This reflects parts of the 'lessons learned' in the article 'Why there aren't more information security research studies' (Kotulic & Clark, 2004). The authors concluded that a survey response rate of 0,61 %, indicated a general mistrust of outsiders collecting data of a sensitive nature, and that firms were unwilling to participate without a strong assurance that the information provided would not harm them (Kotulic & Clark, 2004: 603-605).

Even though I did not experience mistrust, some authorities had reservations concerning which data they were comfortable with having published, especially if it was connected to their role or spokesperson for their employer. To avoid any concerns, interviews with authorities were only conducted in the pilot study and used as background knowledge to inform further research. Based on both ethical and security considerations, individuals have been anonymised such that readers should not be able to identify individuals in the material. In relation to this, my colleagues and I have had an ongoing dialogue to evaluate which data should be presented or omitted in articles and other forums.

There are two important considerations guiding data protection in this project: research ethics and security of the power supply. Due to this, my main supervisor was requested to sign a non-disclosure agreement before transcripts and material from interviews were shared. To ensure data protection, I used my company email address and computer to engage with the industry and to store recordings of interviews and transcriptions where individuals or companies could be identified. This meant that I could offer the same level of data security as we offer our customers. For interviews and transcripts where individuals or companies could be identified, additional measures to protect data were taken. Recordings were not stored at personal equipment, but directly on the company equipment or a dictaphone. Moreover, folders with access control were used to store recordings of interviews. The data management plan, data collection, and interview guide were discussed with key personnel in the company and approved by the data protection officer. The data management plan was also submitted to and approved by the Norwegian Research Council.

Regarding research ethics, I believe that transparency concerning intention and role is an important step. I choose to wear my two hats as consultant and researcher openly. In smaller fora where observations were planned, such as industry preparedness exercises, I and/or a colleague would inform the participants of my employment, the

research project, and that I was there to observe and learn. In larger fora, such as industry conferences, I sometimes put 'PhD student' down as my title, when suitable.

My closeness to the industry exposed me to some 'colourful' metaphors surprisingly suited to enrich my understanding of the industry, challenges, and concerns. One claimed there was a "digitalisation frenzy" in the industry where increased cyberrisk is no longer a choice, but rather a consequence of a digitalisation 'forced' on them by authorities or the management (e.g., smart meter and cloud solutions). Another reminded me that no matter how important cyberrisk is, the main concern for supply of electric power is the "two terrorists in the Norwegian power supply: men with excavators and God." This highlights the two important reasons for down-time in distribution of electric power, namely by accident or the weather conditions. Furthermore, I learned that there are alternative strategies to operate, for instance "disaster-based maintenance", which should be interpreted as the complete opposite to resilience and a possible strategy when preventive measures are seen as unrewarded.

4 OVERVIEW OF ARTICLES

Having outlined how research questions were generated through an interactive approach and methods used, this chapter provides an overview of the dissertation articles, as summarised in the table below.

	Article 1: **Regulations**	Article 2: **Openness**	Article 3: **Foresight**	Article 4: **Strategy**
RQ	How are cyberrisk regulations perceived and translated into internal routines?	How can openness contribute to understanding cyberrisk?	How may scenario analysis improve cybersecurity?	How is ransomware organised as business models and what are their building blocks?
Theory	Risk appetite	Known and unknown risks, Johari's window	Scenario analysis (foresight)	Business models
Method	Case study	Content analysis	Conceptual discussion	Content analysis
Key findings	Although most are positive towards cyberrisk regulations, some feel 'paralysed' by the task and the majority request clearer guidelines, which may minimise workload.	Different actors provide conflicting and vague descriptions of risk. Openness is the intention, but not the practice.	Foresight as a "risk radar" may challenge mental models, promote early detection of risks and learning. Possible challenges are boundary-work, self-fulfilling prophesies and a 'paranoid organisation'.	Four types of ransomware business models are identified as: *door-to-door*, *direct export*, *lock-in* and *platform*. Some of these are organised as franchises.
Conclusion(s)	The translation process is characterised by high workload, uncertainty concerning intended measures and perceived complexity of cyberrisk.	Two-way openness may improve understanding of risks both directly and by "combining the pieces" to make unknown risks known.	Scenario analysis may increase an organisation's knowledge of cyberthreats.	Variations in ransomware attacks can be explained by the attacker's strategic choice of customer segment and value proposition.

Table 4 Overview of articles

The attached articles explore how cyberrisk can be interpreted, defined, and understood through the four different perspectives of: regulations, openness, foresight, and strategy. Article 1 (regulations) studied how external cyberrisk regulations are perceived and translated into internal routines. The article was based on empirical data from the Norwegian electric power industry and highlighted the challenges that the industry faced in this translation process. Article 2 (openness) provides a definition of cyberrisk, identifies the dominating cyberthreat for Norwegian companies and presents a model for how communication and openness may improve the situational awareness and cybersecurity. Article 3 (foresight) problematises how and why traditional risk management fails to manage cyberrisk. Instead, foresight, in particular scenario analysis, is proposed as a tool to address uncertainty, decrease vulnerability, and improve cybersecurity. Article 4 (strategy) applies the business model canvas as a framework to describe, analyse and compare four cases of ransomware attacks. The article demonstrates variation in attacks and provides a systematic approach to analysing attacks.

4.1 Article 1: Regulations

Title: "Just tell us what to do": Regulations and cyber risk appetite in the electric power industry[2]

Regulations are one of the layers applied to ensure a safe and resilient power supply. When the *preparedness regulations* in Norway were updated in 2019, the main changes were concerning cybersecurity. The preparedness regulations mainly contain qualitative criteria and impose the electric power companies to define risk acceptance criteria. For instance, several paragraphs instruct the companies to conduct risk assessments and implement respective measures, typically internal routines. Previous research has shown that the electric power companies and the authorities rank threats

[2] Aakre, S. (2020). "Just tell us what to do" Regulations and cyber risk appetite in the electric power industry. In P. Baraldi, F. Di Maio, & E. Zio (Eds.), *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*. Research Publishing, Singapore.

and efficiency of routines differently (Røyksund, 2011: 45, 48). This indicates that external regulations might be given a higher or lower priority than that intended by authorities. Moreover, given the high degree of autonomy in the regulation regime, little is known about the process in which external regulations are adapted into internal routines.

This article investigated how electric power companies translated external regulations into internal routines. The author followed a project group with representatives from six electric power companies, an industry association, and external consultants. The aim of the group was to operationalise the regulations into routines to be implemented in each electric power company. Data from interviews and observations were gathered over a period of six months in 2019. Secondary data were used as background information and as a supplement to the findings. The research revealed a substantial workload related to interpreting and fulfilling the qualitative regulations concerning cybersecurity. The project group first discussed the regulations to identify documents, templates and routines needed. Afterwards, they gathered and adapted routines and documents previously used by the individual companies and developed new material where needed. The project group spent an estimated 800 hours interpreting the requirements in the regulations, preparing templates and internal routine documents, before risk assessments were conducted and measures implemented in the individual companies.

Cyberrisk is perceived as a complex topic, which explains why the majority requested clearer regulations and guidelines. Even though a set of guidelines were published, it was still unclear to the group how certain paragraphs in the regulations could be fulfilled in practice. The complexity of cyberrisk combined with somewhat 'unclear' guidelines, and the substantial workload for their assessment, caused some to feel 'paralysed' by the task of translating external regulations into internal routines because they did not see a beginning or end to the process. This is a challenge in risk management, especially in cyberrisk, as the risk environment develops continuously.

Despite the critique against the authorities, the industry was generally positive towards regulations concerning cybersecurity. This was because they were concerned about the risks and saw how regulations both increased attention to the subject as well as gave legitimacy to investments in personnel and technical solutions.

4.2 Article 2: Openness

Title: Which cyberthreats do Norwegian companies face, and how can openness contribute to understanding cyberrisk?[3]

Relevant information can be considered a prerequisite in a risk management process. As cyberrisks can be particularly challenging to identify and understand due to their intangible nature, companies may seek information and advice from external risk assessments and threat reports. This article analysed seven open risk assessment and threat reports published in 2018 and 2019 by Norwegian authorities and initiatives addressing cyberrisk. Content analysis demonstrated which cyberthreats were seen as dominating, and how they were communicated. 14 categories of cyberthreats were identified as most prominent, due to the frequency by which they were addressed in the majority of the reports. The cyberthreat categories included: network operations, compromises, reconnaissance, phishing, foreign intelligence, malware, sabotage, espionage, exploitations, ransomware, denial of service, hijacking, influence operations, and insiders. Even though overarching cyberthreats are found, some reports provide conflicting views on the cyberrisk situation and use vague descriptions, which may limit their usefulness to companies.

Openness is a recurring theme in the analysis. The reports showed a broad consensus concerning the importance of cooperation, openness and information sharing in minimising cyberthreats. This is welcomed by the companies. Openness seemed to be the intention from both authorities and companies, however, they faced challenges in practice, and there was a lack of information sharing from both sides. On the one hand,

[3] Aakre, S. (2020). Hvilket trusselbilde står norske virksomheter overfor, og hvordan kan åpenhet bidra til å forstå cyberrisiko? *Magma, 20*(2), 18–26.

increased information sharing from the authorities was requested. On the other hand, few cyber incidents were reported to authorities. Both authorities and companies faced a dilemma of information sharing. The authorities had to balance whether information sharing was justified from a point of national security and the risk of misuse. Whilst companies faced a similar dilemma in situations with cyberattacks or data breaches. Information sharing can help prevent further attacks, but the company might face reputational and financial loss.

A model based on Johari's window and theory of known and unknown risks was developed to illustrate how two actors respectively hold a known and unknown 'portion' of e.g. a situation, phenomenon or risk. Applying information sharing as an example, the model showed how the actors' understanding of the overall situation would expand. The model also illustrated the potential of two-way information sharing to reveal previously unknown risks. Furthermore, this article offers a new definition of cyberrisk as 'values at stake through digitalisation'. It is specified that the values can be of 'material and immaterial nature', and the risk may arise both 'intentionally and unintentionally'.

4.3 Article 3: Foresight

Title: Foresight as risk radar: How may scenario analysis improve cybersecurity?[4]

A common critique of traditional risk management systems is that they are reactive in nature. Several risk management frameworks and internal control systems, as well as technical intrusion detection systems, are based on historical data. The risk management systems are often used to expose incidents after they have occurred, and even the 'proactive' risk management is sometimes characterised by routine-based 'box-ticking'. This might give inaccurate, or in the worst case, misleading predictions about the future. A reactive approach to risk management is believed to be unfit for

[4] Bourmistrov, A. & Aakre, S. (2020). Framsyn som risikoradar: Hvordan kan scenarioanalyse forbedre cybersikkerhet? *Magma, 20*(2), 55–61.

managing cyberrisk, as they might emerge in new forms and fashions. However, the challenge is: how to gain knowledge about risks that have not yet occurred?

The article offers a conceptual discussion of whether foresight and scenario analysis may improve an organisation's cybersecurity and decrease vulnerability. Developing scenarios is a method to acknowledge that the future is uncertain and raise awareness about 'potential futures'. The risk radar is used as a metaphor for how the foresight method allows the combination of proactive 'scanning' of the environment and 'zooming in' on specific scenarios, events or risks in the future. It is demonstrated that the method might balance out an *illusion of control* created by traditional risk management systems and be more effective against 'black swans'. This is because scenario analysis aims to challenge existing mental models, is designed to stimulate attention to potential threats, and is a tool for continuous learning. Developing scenarios may aid the development of contingency plans and prepare for unknown future risks.

It is important to be aware of potential dilemmas and pitfalls when applying scenario analysis. These may create problems for practice and require future research for clarification. Three dilemmas are identified and addressed in this article. These are organisational boundary-work, self-fulfilling prophesies, and a 'paranoid organisation'. First, organisational boundary-work raises the dilemma of who should be involved in generating scenarios, for which the possibility spans from a narrow, internal circuit to crowdsourcing. The alternatives demand different costs and resources, responsibility, autonomy and raises ethical dilemmas. A self-fulfilling prophesy, the second identified dilemma, arises if the anticipation of a given scenario affects collective action to an extent where it increases the likelihood of that scenario occurring. This may occur if attention is devoted to a particular scenario from internal and/or external actors. For instance, exposing vulnerabilities to external actors might increase the likelihood of exploitation by criminal actors. Finally, a 'paranoid organisation' is used to describe a situation with excessive attention to unfavourable

scenarios and a concern that the scenario will occur. This may generate delusions about risk and related mistrust and suspicion. Similarly, favourable scenarios may be disregarded and excluded from the organisation's contingency plans and routines.

4.4 Article 4: Strategy

Title: Ransomware as business models[5]

Ransomware, the encryption of files and a ransom demand in order to decrypt, is one of the most damaging types of cyberattacks. Attacks bring about substantial economic loss and threaten the functioning of society by damaging services, supply chains and critical infrastructure. It is widely acknowledged that ransomware attacks are typically conducted as profit-generating activity for cybercriminals. However, the business side of ransomware is understudied as current research mainly devotes its attention entirely to technical solutions. Business model theory is well suited to examine and describe how an enterprise creates, delivers and captures economic value. This article aimed to demonstrate how ransomware attacks are organised as business models. Deductive content analysis was applied to analyse four ransomware cases based on the 'building blocks' of the business model canvas.

The article presented variations in business models behind ransomware attacks. These variations could be explained by the two factors *customer segment* (targeted vs mass market) and *value proposition* (single vs multiple). The constellation of customer segment and value proposition should be interpreted as strategic choices made by the attackers on how to operate their business. A matrix illustrated the four identified ransomware strategies: *door-to-door*, *direct export*, *lock-in* and *platform*. Moreover, the use of *franchising* was found to have become an important factor in leveraging and operating ransomware business models more effectively. The analysis divided the 'building blocks' of the business model into *core*, *comfort* and *competitive* factors. The core factors are necessary to operate the business model and cannot be replaced. In

[5] Aakre, S. (2022, preprint). Ransomware as business models.

other words, without these core factors, there is no ransomware business model. The comfort factors are necessary but can be replaced without fundamentally changing or disrupting the business model. The competitive factors are comfort factors applied in such a way that it makes one business model more effective than another. It is the competitive factors that differentiates ransomware business models.

Insight into how cybercriminals operate is crucial for interpreting challenges and for designing effective countermeasures. The findings of this article challenge previous studies by differentiating complex business models from 'script kiddies', challenging the use of the Ransomware-as-a-Service term, and suggesting a reassessment of the role of trust in ransomware transactions. 'Business modelling' ransomware offers a systematic approach to analysing and interpreting the challenge. This article offers an examination of the complex issues of ransomware attacks through an easily comprehendible and well-known framework. This can help managers conceptualise and understand the current dominating cyber-dependent crime, ransomware. The proposed method can be useful for communicating cyberrisk to, e.g. managers and board members, and to test, discuss and analyse the effectiveness of countermeasures.

5 DISCUSSION

This chapter combines the findings in the dissertation articles with the theoretical framework presented in chapter 2. Figure 2 below, illustrates how this analysis is done. The four perspectives for interpreting cyberrisk in the articles, are supplemented with additional literature and relevant examples, and together are applied to discuss global cyberrisk in relation to Beck's typology of manufactured risks (5.1). These combined, elaborate on the intangibility of cyberrisk as de-localised, incalculable, and non-compensable (5.2).

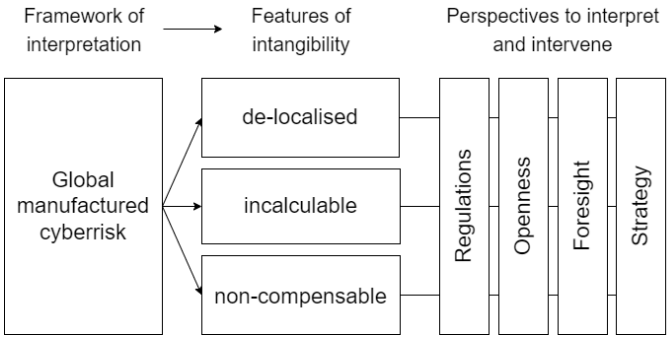


Figure 2 Overview of discussion

Section 5.3, 5.4 and 5.5 draw on the articles constituting this dissertation to discuss how to move beyond intangibility and localise, visualise, and prevent cyberrisk. Lastly, section 5.6 presents a summary of this discussion and its contributions to the field.

5.1 Global manufactured cyberrisk

The digital revolution which started from around the 1950s, has reformed society (Giddens & Sutton, 2021: 5) and brought us into a "new chapter" of the risk society (Beck, 2013). The victory of digitalisation follows the paradox of the risk society, and unintentionally produced cyberrisk. To exemplify: the idea of "man-computer symbiosis" and artificial intelligence was a vision of improved thinking, problem solving and decision making (Licklider, 1960). However, numerous examples have shown that artificial intelligence tends to be biased, reproduce a lack of diversity, and

discriminate against minorities (UNESCO, OECD, IDM, 2022: 50-52). The pacemaker saves lives by ensuring the regularity of the heartbeat. However, it is possible for the signals to be hacked to deliver deadly electric shocks (Jack, 2013).

The internet has revolutionised society and opened numerous possibilities for e.g. communication, entertainment, public services, and critical infrastructure. However, the flip side of the coin to this connectivity dream, is the cyber nightmare. The openness dilemma in cyberspace is that, every new connection makes a network valuable, but also vulnerable. The storage of customer data in an app for a customer loyalty program also opens the possibility for a data breach for example. Or monitoring an aquarium in a casino, can serve as a way in for hackers (article 2). Digitalisation's omnipresence in society makes cyberrisk truly global. Digitalisation may be beyond the point of no return, and in practice, no longer a choice at an individual, organisational or societal level. For instance, the introduction of the smart meter in every household was imposed by the authorities despite its related risks, and the worst-case scenario of massive blackouts (article 1). Unlike King Midas and the 'golden touch', we cannot simply ask to be relieved of the 'cyber touch'. We are the mother of the 'cyber touch', but without the power – and perhaps will – to reverse the impact of the goods and 'bads'.

Although there are numerous examples of how cyberrisk can be seen as following the logic of technological advancement and unintended side effects, cyberrisk also differs from other global manufactured risks. The following discussion on these similarities and differences is based on Beck's typology of global risks[6] (Beck, 2002: 43-46; 2009a: 13-14, 199-204). Beck's work addresses some key distinctions between ecological risk, financial risk, and terrorism. The typology is, of course, idealised (Rasborg, 2021: 7), and the distinctions are meant to systematise and explore interrelations (Beck, 2009a: 13). The following distinctions between risks should therefore not be interpreted as

[6] In Beck's later works also addressed as uncertainties

'absolute', but as a way to systematise and discuss cyberrisk in relation to other global risks. The three distinctions presented here are *cause*, *origin*, and *harm*.

First, *cause* reflects the logic of goods and 'bads' where risks are unintended side effects, such as ecological risk and financial risk. As discussed, cyberrisk, such as increased vulnerability and system errors, 'fit the bill' as an unintended side effect of digitalisation. The distinctions here become evident when considering terrorism, where the unintentional is replaced by the intentional (Beck, 2002: 43-44). Terror is not caused by accident, but intent. However, cyberrisk can also be intentional, such as cyberattacks, as discussed in articles 2 and 4. Cyberrisk entails both the characteristics of the unintended and intended effects.

Second, the *origin* of risk concerns whether it is seen as originating from 'outside' or 'inside' of social structures. Where ecological risk is an example of the prior, financial risk is an example of the latter (Beck, 2002: 43). The origin of cyberrisk is challenging to 'locate' because cybernetic reproduction displaces the boundaries of risk between real and virtual (van Loon, 2000). In addition, the physical sphere and cybersphere are intertwined. Cyber is increasingly seen as an "extension" of the material world (Giddens & Sutton, 2021: 5-8). However, following the divide in origin, network and system failure can be interpreted as examples of cyberrisk originating from 'outside' of social structures. Furthermore, cyberrisk can be placed 'inside' social structures, such as user error, social manipulation or propaganda. Hence, cyberrisk originates from both.

Third, risk concerning the distribution of *harm* as either individual or systemic varies. While financial risk can impact individuals in similar situations very differently, ecological risk is closer to a systemic distribution. Cyberrisk incorporates both of these characteristics. On the one hand, cyberattacks typically cause individuals or organisations harm. On the other hand, cyberrisk can cause systemic or collective harm, such as undermining democracy through fake news and misinformation campaigns

or disrupting critical services through large scale supply chain attacks. Furthermore, the speed of acknowledgement for cyberrisk varies. Risks perceived as individual tend to be more 'immediately' noticeable, like financial risk (Beck, 2002: 43). While a cyberattack may be quickly recognised, the future repercussions of artificial intelligence, cryptocurrencies, and 'internet of things' remain unknown. The discussed cause, origin, and harm of risks, are summarised in Table 5 below.

	Ecological risk	Financial risk	Terror	Cyberrisk
***Cause* of risk**	Accident	Accident		Accident
			Intent	Intent
***Origin* of risk**	Outside			Outside
		Inside	Inside	Inside
***Harm* of risk**	Systemic		Systemic	Systemic
		Individual		Individual

Table 5 Typology of global manufactured risks

Because cyberrisk is multi-faceted, a broad definition of cyberrisk is needed. This dissertation builds on the following understanding, and proposed definition of cyberrisk:

> *"Cyberrisk is values at stake through digitalisation. The values may be of material and immaterial nature, and the risk may arise both intentionally and unintentionally."* (article 2, own translation)

This definition connects cyberrisk directly to digitalisation. However, digitalisation does not cause cyberrisk per se. Digitalisation becomes risk when it interferes with values. Value is socially constructed and does not necessarily represent an objective price or assessment, but something of human importance (objects, constructs or individuals) – material or immaterial. As such it should be interpreted as something of human value, including humans themselves (Rosa, 1998: 28). To exemplify, material values may be machines, systems and physical assets, and immaterial values may be sensitive personal data, intellectual property, or reputation. Furthermore, the risk may

either arise intentionally, like cyberattacks and espionage, or unintentionally, like mistakes and error in systems or human action.

To summarise, cyberrisk should be interpreted as the archetype of global manufactured risks of our time. Having outlined how manufactured cyberrisk is multifaceted – and arguably more so than comparable global risks in the risk society – this may serve as an explanation for why cyberrisk is perceived as complex and intangible (article 1). Interpreting cyberrisk as a global manufactured risk implies intangibility. The following section will therefore address the three features of intangibility: de-localisation, incalculability, and non-compensability in relation to cyberrisk.

5.2 Intangibility of cyberrisk

Digitalisation and connectedness make cyberrisk **de-localised** in terms of borders, causes and consequences, and even time. Examples of de-localisation in terms of borders can be found in article 4 which discussed cybercriminals reaching targets independent of national borders or established business connections. In this case, the advantage of digitalisation is asymmetric, as traditional institutions tend to be bound by borders and the rules of the industrial society. For instance, while cyberattacks are 'borderless', legal jurisdictions are bound by national borders or international cooperation and agreements in order to prosecute cybercriminals. The nature of cyberrisk and connectedness also contributes to dispersing risk. For instance, it is possible to clone computer programs and codes, to adapt and use them multiple times. Cyberrisk therefore can be persistent. The persistence is connected to de-localisation in time and latency because an attack today does not exclude an attack tomorrow, or vice versa.

De-localisation is fuelled by digitalisation and globalisation. The internet's truly global character enables the development of complex supply chains, systems, and network connections, at a pace where managers no longer have an overview. Furthermore, this

interconnectedness means that attacks, system errors, or human actions, can pose consequences for any component or actor in the network. On the one hand, when relating cyberrisk to digitalisation and the development and expansion of ARPANET in the 1970s, we may say that cyberrisk has a long latency. On the other hand, cyberrisk is often argued to be characterised by quick changes and rapid growth. Even though this sounds like two opposites, it may help to summarise a key concern related to de-localisation of cyberrisk (as briefly addressed in section 3.1). That is, we do not know within which borders (where), the consequences (what), the cause (why/how), the time (when), or even whether (if) the risk will manifest itself. Cyberrisk is latent within systems, structures, networks, and connections. The incident might have occurred already, we might experience a cyberattack tomorrow, or an unknown unknown (articles 2 & 3) in the future.

The intangibility and de-localisation of cyberrisk is linked to the **incalculability** of cyberrisk. How can cyberrisk be calculated in a meaningful way to guide decision-making when we do not know where, what, how, when or even if an event will occur? Calculation in traditional risk assessments typically means probabilities (Aven, 2016: 8), a function that with some degree of certainty can predict the likelihood of an event. For instance, to calculate future risk derived from previous events and forecasting. This approach to calculation depends on knowledge of previous events, such as incident reporting and monitoring systems providing data and statistics. A challenge for the calculation of cyberrisk and cybercrime is significant historical data limitations since incidents often go unreported (Kosub, 2015: 631; Maimon & Louderback, 2019: 208). This is one of the key challenges discussed in article 2.

There are at least three dilemmas to consider in the search for information to improve calculation. First, organisations and governments may be hesitant to share information about cyber events because of reputation, resource demand, and practical inconvenience (article 2). Second, sharing sensitive data is balancing on the knife's edge of whether security is better maintained by secrecy or openness (article 2). This

is related to the question of 'to what end' do we wish to calculate. Third, even if we did have 'perfect' statistics, the challenge of calculating or forecasting cyberrisk, is that historical data and emphasis on the past may be a poor indicator of the future (articles 2 & 3). This is related to the concern of our inability to predict future risks, which is particularly true for unknown unknowns, and that the intangibility of cyberrisk is fuelled by de-localisation and incalculability.

The feature of **non-compensability** is typically operationalised as insurability. There are two main arguments for non-compensability: incalculability, and the severity and irreversible nature of the effects. Incalculability here means the limited access to data on loss and exposure to establish a cyberrisk insurance market (Peters et al., 2018: 27). Another complication for insurability is the question of what would constitute a 'fair' compensation to cyberrisk. Digitalisation has reformed traditional structures in society to the extent that cyberrisk has entered the sphere of risks to fundamental human rights. For instance, Edward Snowden's exposure of classified national surveillance programs (National Whistleblower Center, 2022) not only limited his personal freedom but raised questions about a 'surveillance society' and "digital freedom risk" (Beck, 2013). On that note, what would be considered 'fair' compensation for rigged elections through algorithm-based propaganda and selective or fake news?

A related concern to non-compensation is irreversibility. Häfele (1974: 313-314), address of nuclear reactor safety, raised the problem that the opportunity to properly test new technology before it is put into use is limited. This is because safety can only be 'reduced' to a laboratory setting as sub-problems, which can only result in an approximation. This makes the real world the 'laboratory' for residual risk of new technology where we will experience its consequences (Häfele, 1974: 313-314; Beck, 1992b: 108). To some extent, virtual clones (often referred to as digital twins), are used in the cyber domain to execute the laboratory test. Although programs, components and systems can be thoroughly tested before launch, the interconnectedness of systems, networks and people, is the 'joker' making consequences unpredictable. In the

situations discussed, it is unclear what a 'real' compensation could constitute for lack of personal freedom, or ripple effects of severe consequences beyond imagination. Additionally, if Ord's (2020: 167-169) estimates are right, what could be considered a fair compensation for a 1 in 10 chance of an existential catastrophe via unaligned artificial intelligence over the next 100 years? The non-compensability of cyberrisk is a challenge beyond calculation and insurance. The irreversibility of the consequences suggests that the important question is how to prevent cyberrisk.

This section has discussed what the three features of intangibility mean in the context of cyberrisk. The common determinator for the intangibility of global risks is the lack of knowledge, or even 'non-knowledge', keeping them de-localised, incalculable, and non-compensable. The changing character of cyberrisk suggests that we need better ways to describe, visualise, and think in terms of risks, to control them (Pentland, 2016: 208). The following three sections explore how managers may move beyond intangibility.

5.3 From de-localised to localisation

The risk society thesis, or world risk society, offers a broad and societal perspective on risks. The manufactured risks in the risk society themselves are global in reach. However, the consequences tend to be local, meaning to some degree possible to observe as for example, cyberattacks or system failure. Even though cyberrisk is characterised by de-localisation, this dissertation shows how it is possible to gain knowledge about cyberrisk through the *local consequences*.

The translation process from external, qualitative regulations, to internal templates, as studied in article 1, is an attempt to adapt external, standardised regulations and global risks to a local level. Derived from the regulations, risks were imagined, assessed, and evaluated based on a local context. This is not to say that the process was 'friction free'. The process clearly caused some frustration, particularly when the requirements in the regulations were perceived as poorly specified, did not fit the local context, or even

considered impossible in practice due to limitations in the technical solution in use. The companies then faced the dilemma of whether to define acceptable risk based on the local context or the external regulations.

While searching for information to inform cyberrisk management, the content analysis of threat reports in article 2, found that information about cyberthreats is not lacking. Instead, their usefulness was questioned since the reports used different terminology and sometimes provided divergent and vague descriptions of the situation. The main obstacle to making the cyberthreats discussed in the reports more tangible, seemed to be related to communication. Licklider and Taylor (1968: 21) highlighted the pros and cons of technology and communication when describing the first "technical meeting held through a computer" 54 years ago. They used simple illustrations from table tennis to show that communication goes two ways and that communication is destroyed if one party bombards the other with ping-pong balls, as shown in Figure 3 below. This is one of the challenges found in article 2. To ensure the usefulness of information, a suggestion for practice is to metaphorically take a place at the ping pong table and play. Participating in the communication can increase the relevance of information and help identify the 'ping-pong balls' which should receive attention as a result of cyberrisk becoming slightly more tangible.

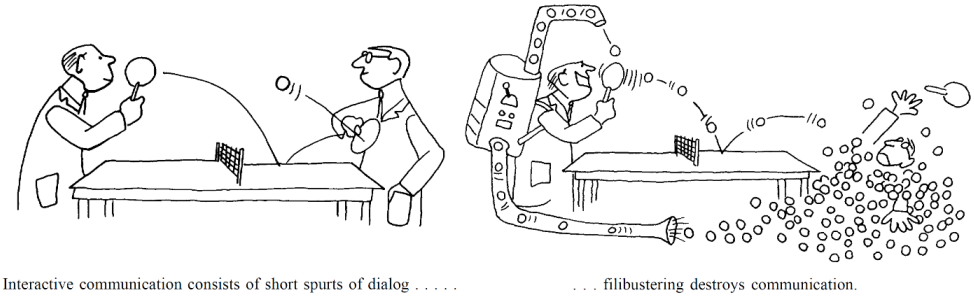


Figure 3 Illustrations of communications (Licklider & Taylor, 1968: 34-35)

An approach to gain knowledge about future risks and unknown unknowns is applying scenario analysis and foresight as a "risk radar" (article 3). Scenario analysis and foresight is a process for developing scenarios, or narratives about what the future

might look like, and how it might impact the organisation's operations. The "risk radar" allows organisations to 'scan' the environment for global trends (e.g., artificial intelligence in the work sphere), emerging threats (e.g., increasing supply chain attacks), or even 'weak signals' (e.g., implementation of blockchain technology in the public sector), and build scenarios that explain the local consequences. Furthermore, as a tool to minimise de-localisation in time, scenarios can be seen as a tool to 'pull' the future closer by producing reliable narratives about what possible futures might look like.

The cyber domain is not only characterised by unintended side effects per se, but misuse of technological advancement for intentional purposes, such as fraud, illegal intelligence gathering, and cyberattacks. This kind of risk has a 'counterpart' that is often de-localised. Article 4 showed how changing the perspective from the focal organisation to a counterpart, can give knowledge into how attacks can manifest themselves on a local level. To address this dynamic, a key consideration for managers is the two-dimensional question 'what makes us valuable – and how does this make us vulnerable?'.

To summarise, the intangibility of cyberrisk can be decreased by using different perspectives to gain knowledge about the manifested and imagined local consequences. This means that the lack of knowledge caused by intangibility and de-localisation can be reduced. Having considered means to localise risk, the new knowledge has implications for the possibility of developing calculations.

5.4 From incalculable to visualisation

In traditional risk assessments, calculation typically refers to probabilities derived from historical data (Aven, 2016: 8). While disciplines such as economics and natural sciences tend to view risk calculation as an objective measure, the social sciences argue for a revised, and broader notion of calculation (Callon & Muniesa, 2005: 1245). This approach opens for different ways of calculating. Applying this principle to cyberrisk

suggests that we can gain knowledge through visualisations e.g., qualitative descriptions and models. Rather than numeric accuracy or model reliability, the importance lies in the communicative and organisational usefulness (Millo & MacKenzie, 2009), as well as its ability to generate pressure for action (Beck, 2009: 86). This dissertation discusses and shows an alternative way of calculating risk, namely by visualisation.

While risk matrixes calculate risk in terms of consequence and likelihood, templates and internal routines visualise risk through descriptions of how a risk may manifest itself, and the courses of action for risk management. The intangibility of cyberrisk suggests that the complexity cannot be captured in probability-based calculations. Qualitative risk descriptions should therefore be considered to serve the purpose of communicative and organisational usefulness. As shown in article 1, the process of adapting and developing templates and internal routine documents, opened for in-depth conversations about risks, and solutions for risk management. In that sense, it served its purpose in terms of communicative usefulness. Nevertheless, templates and routine documents are simplifications that standardise risk management, and may ignore outliers or events assumed to be less likely. Consequently, templates and internal routines may provide limited 'organisational usefulness' in managing risks that do not 'fit' the template.

Information sharing has proven to be challenging in practice. Additionally, the value of information and examples can be questioned if the 'worrisome' risks are expected to be unique or unknown unknowns. As demonstrated in article 2, openness can improve our understanding of a risk situation by providing examples of what the risk might look like. This can be a starting point to explore unknown risks, improve decision making and prevent risk. Openness and information sharing can contribute to consensus on key terminology such as, 'incident', 'risk', 'attack', and 'critical', and also improve situational awareness of cyberrisk within an organisation and between actors (article 2).

Both articles 2 and 3 tap into how unknown cyberrisk can be explored using different approaches. Whereas information sharing provides specific examples, foresight and scenario analysis is a more open-ended approach which can provide insights beyond information sharing. Scenarios are visualisations of potential futures, not meant to predict the future. The process is primarily qualitative, and therefore suited to describe scenarios that are not possible to model quantitatively or calculate. Scenarios can be powerful visualisations to fuel a discussion of the future, including risks. However, the scenarios are only as good as the minds developing them, and generating meaningful visualisations are dependent on involving the 'right' people in the process. The opportunity to involve different stakeholders is a strength with scenario analysis, and the possibilities span from a narrow circuit to crowdsourcing. In addition, the process of developing scenarios, challenges the participants to understand complex causal effects.

In article 4, a business model framework is used to visualise how cybercriminals operate to generate profit. This helps explain the motivation and the mechanisms behind the risk. The business model framework provides visualisations as such, but more so a basis for discussing and evaluating risk. Framing cybercrime as a business problem and not only an IT problem, provides the opportunity for a broader group to take a more meaningful part in the discussion. Interpreting profit-motivated cyberattacks as holistic business models and strategies, is a method to investigate the mechanisms of cybercrime, and its likely developments based on profit-maximising. Furthermore, using a well-known framework can be fruitful in communicating cyberrisk more effectively among e.g., authorities and organisations, and within organisations, to managers and board members.

Beck (2006), 'warns' that calculations of manufactured risks may lead to anticipation of the "wrong" risks. Similarly, a concern with the discussed visualisations of cyberrisk is that they may lead to 'tunnel vision'. This involves one, or a selected number of visualisations receiving a disproportionately high importance and power, to an extent

where alternative visualisations are no longer considered. For instance, scenario analysis aims to challenge mental models to increase learning. If not successful, scenario analysis may replace an illusion of control from traditional risk management systems, with a different state of narrow-minded organisation, like an organisation that experiences 'paranoia' or is biased, towards self-fulfilling prophecies (article 3). Furthermore, if business models are used as a set typology of ransomware attacks, they are likely to be outdated and 'wrong' in the future. This implies that the mechanisms causing business models and strategies to vary, and the core factors explaining the development, are ignored (article 4). It is important to pay attention to the variations and likely developments, to avoid 'tunnel vision'.

Drawing on organisational theory and a broad notion of calculation, visualisations can be generated to facilitate understanding and communication of cyberrisk. Visualisations can serve as a way to discuss risk meaningfully and address potential harm and compensation.

5.5 From non-compensable to prevention

The logics of calculation and compensation are closely connected. However, the ability to calculate risk is only one side of compensation. The other side is related to whether or not it is *possible* to compensate for the loss, e.g., irreversible harm. When risks are non-compensable, 'more compensation' is not a solution. Instead, the risk should, if possible, be prevented from taking place. To avoid risk, attention can be devoted to prevention and precaution (Ewald 1993: 221, 2002: 294-299).

Risk assessment is intended to identify risk as the first step in a risk management process. Assessing and managing the 'omnipresent' cyberrisk, suggests both technological and organisational measures, including training and awareness of personnel. A critical dilemma is the acknowledgement that although extensive measures are taken, cyberrisk is not eliminated (article 1). This means that it is necessary to establish risk acceptance criteria or a 'sufficient' security level. As article

1 showed, the industry felt that they lacked guidance in terms of how to interpret the regulations, and in particular, what would be considered 'sufficient' prevention and 'acceptable' risk. Considering the challenges to 'navigate' between complex risk and unclear regulations, and the substantial resource demand, there was a surprisingly positive attitude towards cyberrisk regulations. This is because the topic was given high importance by the industry representatives. They explained how regulations functioned as an important 'push' toward better cybersecurity as they helped to place cyberrisk 'on the agenda', legitimise new measures, and raise funds and investments in cybersecurity, to prevent and prepare for future attacks.

Although there are data limitations concerning cyberattacks, data we do have, suggests that there is room for prevention if information sharing and openness are utilised. Rather than focusing our attention on preparedness and crisis management alone, we can aim to intervene and minimise risk. Article 2 discussed how Hydro's openness regarding the ransomware attack they suffered in 2019, made it possible to prevent future attacks from the same criminal group. The publicity can also be seen as a tool to raise awareness beyond the particular modus operandi of the criminal group. These are direct results of openness. The attack on Hydro, suggests that there are windows of opportunity to minimise negative consequences and to contain risk, as the initial attack on Hydro took place 3-4 months before the attacker's encryption software was executed. Data we have, indicates that the average time to identify a data breach in 2021 was 212 days (IBM, 2022: 22), which gives a wide window of opportunity to reduce or avoid further consequences. If we can reduce the time to identify risk, it can help contain risk. The challenge is to identify the window by knowing what to look for. Here, information sharing can have an important role. However, when facing unknown unknowns, or 'black swans' other tools to investigate risk can be important to supplement the work.

For instance, article 3 discussed how unknown cyberrisk can be explored using scenario analysis. Developing scenarios is suggested as a tool to discover unknown

unknowns, explore what to prevent, as well as to promote flexibility in terms of preparing for different futures.

> *"Don't fight in the North or the South. Fight every battle everywhere, always, in your mind. Everyone is your enemy, everyone is your friend. Every possible series of events is happening all at once. Live that way and nothing will surprise you. Everything that happens will be something that you've seen before."* (Fictional character Petyr "Littlefinger" Baelish)[7]

The quote, although fictional and from a situation of war, explains how imagining likely and unlikely scenarios can improve flexibility and preparedness. Yet, our 'advisor' Petyr Baelish, made one critical assumption, perhaps the one that cost him his life, which was that complete knowledge is possible. The idea of unknown unknowns is to acknowledge that information is incomplete, and that there are gaps in our knowledge which we might be unaware of (Rumsfeld, 2010). As discussed in article 3, developing scenarios depends on the group's knowledge, and the process, which can include and reproduce biases. There are also ethical dilemmas to consider when deciding the group members, such as whether, or alternatively how to include views of competitors or (ex-)criminals.

Understanding a counterpart's business model and strategy provides knowledge about the typology as well as its strengths and weaknesses. For instance, if we expect 'traditional' ransomware attacks, a securely stored backup is a suited antidote. In this case, the risk of irreplaceable harm is reduced. The knowledge about what to expect gives indications for how to prepare and how to prevent attacks. Understanding cybercriminal's business models and strategies, can therefore contribute to knowledge in predicting the types of attacks to expect based on the evaluation of an attacker's business model.

[7] Benioff, D. & Weiss, D. B. (Wrs.) (2017, SE7, EP3). The queen's justice. [TV series] *Game of Thrones*. HBO.

Prevention and precaution are challenging in practice, not only because of the suggested nature of risk which cannot be eliminated, but also because successful prevention of risk can lead to the preventative measures being questioned. Prevention can be understood as an aim to control the future, and to avoid a situation from occurring. The success of prevention can therefore be measured as the absence of change or incidents. A further question is whether the absence of incidents can actually be attributed to the preventive measures or external factors, coincidences or 'luck'. However, absence of incidents may, in reality, reflect that risks, near misses, or incidents, are simply not registered. Successful prevention or limited data may support the idea that nothing is happening. Consequently, the preventative measures can be interpreted as invaluable or unnecessary, which may lead to less investments in cybersecurity. This can reflect different views of cyberrisk and risk management practices, such as an 'illusion of control' or 'disaster-based' maintenance and measures.

To summarise, relevant knowledge can help prevent cyberrisk. However, this discussion has also addressed that eliminating risk is not a complete science with permanent solutions.

5.6 Summary and contributions

The discussion builds on the risk society thesis and argues that cyberrisk should be interpreted as the archetype of global manufactured risks. However, interpreting cyberrisk in this frame implies that the risks are de-localised, incalculable, and non-compensable, which is contested in the risk society and problematic for management. Therefore, this dissertation explored four perspectives to intervene with intangibility: regulations, openness, foresight, and strategy. The three features of intangibility are turned inside out to *localise*, *visualise,* and *prevent* cyberrisk, as illustrated in the Figure 4 below.

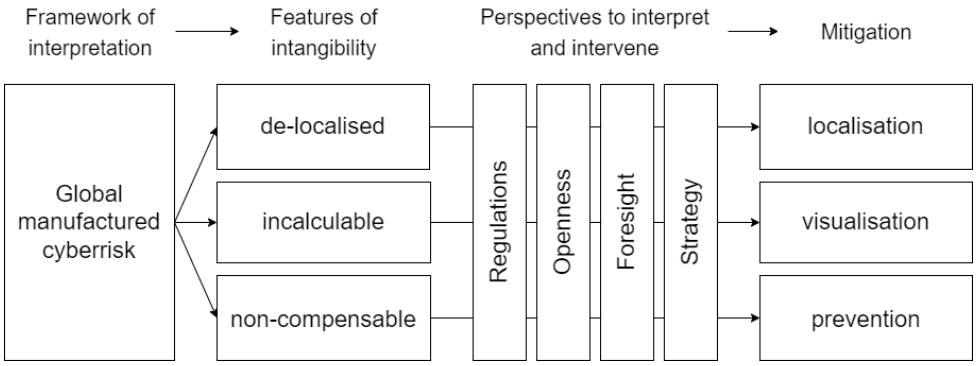


Figure 4 Overview of dissertation

Others have questioned and challenged complete intangibility on both theoretical (Gross, 2016), and empirical grounds (Ericson & Doyle, 2004). Instead, this dissertation studied the implications and suggested four perspectives on how to intervene with intangibility. As elaborated in the articles, regulations, openness, foresight, and strategy, all have their strengths and limitations. However, combining two or more perspectives builds on the principle of triangulation and aims to reduce biases and misinterpretations. Consequently, other perspectives may be useful to entangle cyberrisk.

The dissertation does not fulfil the 'management dream' of turning cyberrisk into something solid. On the contrary, the articles in this dissertation show how cyberrisk resembles an intangible gas state and highlight the dilemmas and challenges for its management. Cyberrisk at a gas state, represents the moving and expanding character of complete intangibility where managers need to always be alert, because management becomes an act of fumbling in the dark. However, because of the intangible character of cyberrisk, knowledge will always have an element of uncertainty. This means the solid state of risk as measurable, and with a constant volume and shape, is likely to represent gross simplifications, anticipation of the 'wrong' risks, and an illusion of control. Instead of chasing the 'management dream' of transforming gas into solid, this dissertation suggests aiming for another state: a

fluid state, something in between a solid and a gas. This fluid state allows us to discuss, address, and mitigate cyberrisk more meaningfully. It allows for rich descriptions without overlooking uncertainty. We move beyond the challenge of non-knowledge to *some-knowledge*, or an approximation of knowledge and what the future(s) of cyberrisk might look like.

Cyberrisk is the archetype of risk in our time, and has the potential to cause severe harm to humanity. The challenge is that both the technical approach to managing cyberrisk, and traditional risk management (Eling et al., 2021; Marotta & McShane, 2018; Articles 2 & 3) are found to be insufficient. This is especially the case when faced with novel cyberrisk, such as unknown unknowns and 'black swans', which are commonly accepted to be dealt with through contingency plans (Refsdal et al., 2015: 123-124). This dissertation contributes to literature in this field by introducing the perspective of *intangibility*, and proposing a different and proactive mitigation strategy: *localisation*, *visualisation*, and *prevention*. The suggested perspectives to intervene with the intangibility of cyberrisk, also demonstrate how localising unknown unknowns can be part of the mitigation strategy. Furthermore, visualising cyberrisk, moves cyberrisk mitigation out of the purely technical sphere to allow for a broader group of organisations to participate in interpreting cyberrisk and intervening with its intangibility on a more meaningful level. Lastly, because cyberrisk has the potential to cause severe harm, attention should be devoted to the prevention of cyberrisk.

Beyond the contributions to interpreting and mitigating cyberrisk, this dissertation contributes to the (world) risk society thesis by extending Beck's (2002: 43-46; 2009a: 13-14, 199-204) seemingly unfinished typology of global risks. It does so by structuring key distinctions (cause, origin, and harm), and including cyberrisk in the typology. Furthermore, instead of rejecting the risk society thesis as a "zombie category" (Gross, 2016), the dissertation presents what the intangibility of cyberrisk may look like. In these ways, the work elaborates on the role and magnitude of cyberrisk in the risk

society, and expands the literature and frame of reference in the cyberrisk society (van Loon, 2000, 2002; Lupton, 2016).

The risk society is concerned with risk, not disasters. Any specific risk ceases to exist as the risk manifest itself, and the risk moves elsewhere (Beck, 2009b: 292). This dissertation addressed the proactive side of cyberrisk mitigation. However, as eliminating cyberrisk is utopic, management of cyberrisk should include a broader spectrum of proactive and reactive measures. For instance, a reactive approach can entail preparedness or resilience as an alternative to compensation.

The relation and differences between risk and uncertainty, particularly with respect to calculation, is discussed in the risk society and addressed in this dissertation. Although the risk society has had impact beyond sociology, the understanding of risk as a 'calculable chance', is still common in other disciplines. If research on cyberrisk builds on the assumption of calculability, it may fail in accounting for intangibility, and also promote a very narrow or possibly wrong understanding of cyberrisk. Research on cyberrisk, as addressed in computer science or information security, may therefore benefit from studying cyberrisk as cyber*uncertainty*, because this concept is less likely to limit the understanding and scope of cyberrisk research.

Managerial implications

As this project emerged from the industry, contribution of knowledge to practice has been a primary goal. Hopefully, this can be seen from the articles which address relevant topics and are written in a way to invite a broader audience to join the conversation. At some levels, the aims of theory and practice intersected, after all, "there is nothing so practical as a good theory" (Lynch et al., 2018). However, to rephrase the question of contribution: can this dissertation offer something solid? The contributions of this dissertation are listed below, with some having reference to the articles where additional information can be found.

- Digitalisation fuels both advantages and disadvantages. (Articles 1 & 2)
- Cyber is only partly technical. Cyberrisk is values at stake through digitalisation, e.g., control systems, personal data, and reputation. The risk may arise both intentionally and unintentionally, e.g., cyberattacks, and human or system errors. (Article 2)
- In a world where cyberrisk feels like omnipresent gas: *localise*, *visualise*, *prevent*.
- Regulations can be helpful to translate risk into a local setting. (Article 1)
- Information sharing and openness among trusted actors is key for a more aligned situational awareness and to prevent cyberrisk. (Article 2)
- Scenario analysis can be applied to complement risk management. (Article 3)
- Cybercriminals are not so cryptic, and we can understand profit-motivated cyberattacks by studying their business model. (Article 4)
- The manager's task is not to eliminate cyberrisk, but to facilitate localisation, visualisation, and prevention.
- The suggestions can be scaled up or down to fit available time and resources. (see e.g., Article 3)

6 CONCLUSIONS

This dissertation has discussed dilemmas, challenges, and intangibility of cyberrisk across its four incorporated articles, and their synthesis in this dissertation as a whole. It has integrated these within the theoretical framework of the risk society thesis. The four qualitative dissertation articles have addressed regulations, openness, foresight, and strategy to define, understand, communicate, and manage cyberrisk from an organisational perspective. Given that intangibility is the main challenge associated with cyberrisk, the overall research question was devised to explore what the intangibility of cyberrisk represents to organisations and how the intangibility of cyberrisk can be mitigated.

The intangibility of cyberrisk was studied by applying Giddens' (2002: 26-29) understanding of manufactured risks, and by extending Beck's (2009a: 13-14) typology of global manufactured risks. The discussion demonstrated that cyberrisk should be interpreted as the archetype of global risks because it is multifaceted and has a truly global character. Interpreting cyberrisk in this frame implies that the risks are *de-localised*, *incalculable,* and *non-compensable*. The findings in the dissertation articles have been discussed in relation to the three features of intangibility and have shown how they can be turned inside out to *localise*, *visualise,* and *prevent* cyberrisk.

Cyberrisk can be localised through templates placing risk in a local context, communication to increase the relevance of information, scenarios to 'pull' the future closer, and understanding the organisation's value to criminals. Cyberrisk can be visualised to facilitate a more meaningful discussion of risk across the organisation. This can be done through qualitative risk descriptions, examples of attacks, scenarios, and cybercriminals' business models. As a result, cyberrisk can be prevented. This is because more targeted measures in cybersecurity can be identified and legitimised, information about risks and incidents can be shared in the 'window of opportunity' to act upon, and the organisation can increase preparedness for different scenarios and

understand which cyberattacks are more likely. Together, this gives organisations possibilities to mitigate intangible cyberrisk.

In conclusion, this dissertation does not claim to have turned cyberrisk from an intangible gas into a solid state. It does however demonstrate how cyberrisk moves between states of intangibility and tangibility, and discusses features of intangibility and the mitigation strategy, including: localisation, visualisation, and prevention. Following this, cyberrisk does not remain in a pure gas state, but becomes a more 'fluid' and thus tangible state.

REFERENCES

Aakre, S. (2020a). Hvilket trusselbilde står norske virksomheter overfor, og hvordan kan åpenhet bidra til å forstå cyberrisiko? *Magma, 20*(2), 18–26.

Aakre, S. (2020b). "Just tell us what to do" Regulations and cyber risk appetite in the electric power industry. In P. Baraldi, F. Di Maio, & E. Zio (Eds.), *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*. Research Publishing, Singapore.

Adam, B. & van Loon, J. (2000). Introduction: repositioning risk; the challenge for social theory. In Adam, B., Beck, U. & van Loon, J. (Eds.), *The risk society and beyond: critical issues for social theory* (pp. 1–31). Sage. https://dx.doi.org/10.4135/9781446219539.n1

Agee, J. (2009). Developing qualitative research questions: a reflective process. *International Journal of Qualitative Studies in Education, 22*(4), 431–447. https://doi.org/10.1080/09518390902736512

Aradau, C. & van Munster, R. (2007). Governing terrorism through risk: taking precautions, (un)knowing the future. *European Journal of International Relations, 13*(1), 89–115. https://doi.org/10.1177/1354066107074290

Arnoldi, J. (2009). *Risk: an introduction*. Polity.

Aven, T. (2014). *Risk, surprises and black swans: fundamental ideas and concepts in risk assessment and risk management*. Routledge.

Aven, T. (2016). Risk assessment and risk management: review of recent advances on their foundation. *European Journal of Operational Research, 253*(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

Beck, U. (1986). *Risikogesellschaft: auf dem Weg in eine andere Moderne*. Suhrkamp.

Beck, U. (1992a). From industrial society to the risk society: questions of survival, social structure and ecological enlightenment. *Theory, Culture & Society, 9*(1), 97–123. https://doi.org/10.1177/026327692009001006

Beck, U. (1992b). *Risk society: towards a new modernity*. Sage.

Beck, U. (2000). Risk society revisited: theory, politics and research programmes. In Adam, B., Beck, U. & van Loon, J. (Eds.), *The risk society and beyond: critical issues for social theory* (pp. 211–299). Sage. https://doi.org/10.4135/9781446219539

Beck, U. (2002). The terrorist threat: world risk society revisited. *Theory, Culture & Society, 19*(4), 39–55. https://doi.org/10.1177/0263276402019004050

Beck, U. (2006). Living in the world risk society: A Hobhouse Memorial public lecture given on Wednesday 15 February 2006 at the London School of Economics. *Economy and Society, 35*(3), 329–345. https://doi.org/10.1080/03085140600844902

Beck, U. (2009a). *World at risk* (2. ed.). Polity.

Beck, U. (2009b). World risk society and manufactured uncertainties. *Iris : European Journal of Philosophy and Public Debate, 1*(2), 291–299.

Beck, U. (2013). The digital freedom risk: too fragile and acknowledgement. *OpenDemocracy (London).*

Beck, U. (2014). Incalculable futures: world risk society and its social and political implications. In Beck, U. (Ed.), *Ulrich Beck: Pioneer in Cosmopolitan Sociology and Risk Society* (pp. 79–90). Springer. https://doi.org/10.1007/978-3-319-04990-8_8

Bourmistrov, A. & Aakre, S. (2020). Framsyn som risikoradar: Hvordan kan scenarioanalyse forbedre cybersikkerhet? *Magma, 20*(2), 55–61.

Bromiley, P., McShane, M., Nair, A. & Rustambekov, E. (2015). Enterprise risk management: review, critique, and research directions. *Long Range Planning, 48*(4), 265–276. https://doi.org/10.1016/j.lrp.2014.07.005

Callon, M. & Muniesa, F. (2005). Economic markets as calculative collective devices. *Organization Studies, 26*(8), 1229–1250. https://doi.org/10.1177/0170840605056393

de Caprona, Y., (2013). *Norsk etymologisk ordbok: tematisk ordnet*. Kagge.

Caygill, H. (2000). Liturgies of fear: biotechnology and culture. In Adam, B., Beck, U. & van Loon, J. (Eds.), *The risk society and beyond: critical issues for social theory* (pp. 155–164). Sage. https://doi.org/10.4135/9781446219539.n8

Cebula, J. J. & Young, L. R. (2010). *A taxonomy of operational cyber security risks*. (CMU-SEI-2010-TN-028). Carnegie Mellon University, Software Engineering Institute.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security, 56*, 1–27. https://doi.org/10.1016/j.cose.2015.09.009

Curran, D. (2015). Risk illusion and organized irresponsibility in contemporary finance: rethinking class and risk society. *Economy and Society*, *44*(3), 392–417. https://doi.org/10.1080/03085147.2015.1044850

Douglas, M. & Wildavsky, A. (1982). How can we know the risks we face? Why risk selection is a social process. *Risk analysis, 2*(2), 49–58. https://doi.org/10.1111/j.1539-6924.1982.tb01365.x

Douglas, M. & Wildavsky, A. (1983). *Risk and culture: an essay on the selection of technological and environmental dangers*. University of California Press.

Easterby-Smith, M., Thorpe, R., Jackson, P. R. & Jaspersen, L. J. (2018). *Management & business research*. (6. ed.). Sage.

Ekberg, M. (2007). The parameters of the risk society: a review and exploration. *Current Sociology*, *55*(3), 343–366. https://doi.org/10.1177/0011392107076080

Eling, M., McShane, M. & Nguyen, T. (2021). Cyber risk management: history and future research directions. *Risk Management and Insurance Review, 24*(1), 93–125. https://doi.org/10.1111/rmir.12169

Eling, M. & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance, 17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122

Eling, M. & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research, 272*(3), 1109–1119. https://doi.org/10.1016/j.ejor.2018.07.021

Elo, S. & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing, 62*(1), 107–115. https://doi.org/10.1111/j.1365-2648.2007.04569.x

Ericson, R. & Doyle, A. (2004). Catastrophe risk, insurance and terrorism. *Economy and Society, 33*(2), 135–173. https://doi.org/10.1080/0308514041000167710 2

Ewald, F. (1993). Two infinities of risk. (B. Massumi, Trans.) In Massumi, B. (Ed.), *The politics of everyday fear* (pp. 221–228). University of Minnesota Press.

Ewald, F. (2002). The return of Descartes's malicious demon: an outline of a philosophy of precaution. (Utz, S., Trans.) In Baker, T., Simon, J. (Eds.), *Embracing risk* (pp. 273–301). The University of Chicago Press.

Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L. A., Wang, S. S., Schmit, J., Thomas, R., Elvedi, M., Maillart, T., Donavan, E., Dejung, S., Durand, E., Nutter, F., Scheffer, U., Arazi, G., Ohana, G., & Lin, H. (2019). Cyber risk research impeded by disciplinary barriers. *Science (American Association for the Advancement of Science), 366*(6469), 1066–1069. https://doi.org/10.1126/science.aaz4795

Flick, U. (2009). *An introduction to qualitative research* (4. ed.). Sage.

Giddens, A. (1998). Risk society: the context of British politics. In Franklin, J. (Ed.) *The politics of risk society* (pp. 23–34). Polity Press.

Giddens, A. (2002). *Runaway world: how globalisation is reshaping our lives* (New ed.). Profile.

Giddens, A. & Sutton, P. W. (2021). *Essential concepts in sociology* (3. Ed.). Polity.

Gross, M. (2016). Risk as zombie category: Ulrich Beck's unfinished project of the 'non-knowledge' society. *Security Dialogue, 47*(5), 386–402. https://doi.org/10.1177/0967010616645020

Hagen, J., Hermansen, O., Toftegård, Ø., Pettersen, J.-M., Steen, R. & Paulen, S. L. (2017). *Regulering av IKT-sikkerhet* (Rapport nr. 26-2017). Norges vassdrags- og energidirektorat. http://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf

Hansson, S. O. (2010). Risk: objective or subjective, facts or values. *Journal of Risk Research, 13*(2), 231–238. https://doi.org/10.1080/13669870903126226

Häfele, W. (1974). Hypotheticality and the new challenges: the pathfinder role of nuclear energy. *Minerva (London), 12*(3), 303–322. https://doi.org/10.1007/BF01102526

IBM. (2022). *Cost of a data breach report 2021*. IBM Security.

Jack, B. (2013, February 25). *"Broken hearts": how plausible was the Homeland pacemaker hack?*. Retrieved 02.06.22, from https://ioactive.com/broken-hearts-how-plausible-was-the-homeland-pacemaker-hack/

Jasanoff, S. (1999). The songlines of risk. *Environmental Values 8*(2), 135–152. https://www.jstor.org/stable/30301700?seq=1

Jorgensen, D. (2015). Participant observation. In Scott, R. A. & Buchmann, M. C. (Eds.), *Emerging trends in the social and behavioral sciences: an interdisciplinary, searchable, and linkable resource*. Wiley. https://doi.org/10.1002/9781118900772

Knight, F. (1921). *Risk, uncertainty and profit*. Houghton Mifflin.

Kosub, T. (2015). Components and challenges of integrated cyber risk management. *Zeitschrift für die gesamte Versicherungs-Wissenschaft, 104*(5), 615–634. https://doi.org/10.1007/s12297-015-0316-8

Kotulic, A. G. & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*(5), 597–607. https://doi.org/10.1016/j.im.2003.08.001

Krippendorff, K. (1989). Content analysis. In E. Barnouw, G. Gerbner, W. Schramm, T. L. Worth, & L. Gross (Eds.), *International encyclopedia of communication* (Vol. 1, pp. 403-407). Oxford University Press. http://repository.upenn.edu/asc_papers/226

Licklider, J. C. R. (1960). Man-computer symbiosis. *IRE Transactions on Human Factors in Electronics, HFE-1*(1), 4–11. https://doi.org/10.1109/THFE2.1960.4503259

Licklider, J. C. R. & Taylor, R. W. (1968). The computer as a communication device. *Science and technology. 46*, 21–41 https://internetat50.com/references/Licklider_Taylor_The-Computer-As-A-Communications-Device.pdf

Line, M. B., Tøndel, I. A. & Jaatun, M. G. (2016). Current practices and challenges in industrial control organizations regarding information security incident management – Does size matter? Information security incident management in large and small industrial control organizations. *International Journal of Critical Infrastructure Protection, 12*, 12–26. https://doi.org/10.1016/j.ijcip.2015.12.003

van Loon, J. (2000). Virtual risks in an age of cybernetic reproduction. In Adam, B., Beck, U. & van Loon, J. (Eds.), *The risk society and beyond: critical issues for social theory* (pp. 164–182). Sage. https://doi.org/10.4135/9781446219539

van Loon, J. (2002). Cyberrisks: telematic symbiosis and computer viruses. In *Risk and technological culture* (pp. 147–168). Routledge. https://doi.org/10.4324/9780203466384

Lupton, D. (2013). *Risk* (2nd ed.). Routledge.

Lupton, D. (2016). Digital risk society. In Burgess, A., Alemanno, A. & Zinn, J. O. (Eds.), *Routledge handbook of risk studies* (pp. 301–309). Routledge. https://doi.org/10.4324/9781315776835-42

Lynch, E. A., Mudge, A., Knowles, S., Kitson, A. L., Hunter, S. C. & Harvey, G. (2018). "There is nothing so practical as a good theory": a pragmatic guide for selecting theoretical approaches for implementation projects. *BMC Health Services Research, 18*(1), 857–857. https://doi.org/10.1186/s12913-018-3671-z

Maimon, D. & Louderback, E. R. (2019). Cyber-dependent crimes: an interdisciplinary review. *Annual Review of Criminology, 2*(1), 191–216. https://doi.org/10.1146/annurev-criminol-032317-092057

Marotta, A. & McShane, M. (2018). Integrating a proactive technique into a holistic cyber risk management approach. *Risk Management and Insurance Review, 21*(3), 435–452. https://doi.org/10.1111/rmir.12109

Massumi, B. (1993). Everywhere you want to be. In Massumi, B. (Ed.) *The politics of everyday fear* (pp. 3–37). University of Minnesota Press.

Mayring P. (2019). Qualitative content analysis: demarcation, varieties, developments. *Forum Qualitative Sozialforschung, 20*(3). https://doi.org/10.17169/fqs-20.3.3343

Millo, Y. & MacKenzie, D. (2009). The usefulness of inaccurate models: towards an understanding of the emergence of financial risk management. *Accounting, Organizations and Society, 34*(5), 638-653. https://doi.org/10.1016/j.aos.2008.10.002

Mythen, G. (2004). *Ulrich Beck: A critical introduction to the risk society.* Pluto Press. https://doi.org/10.2307/j.ctt18fs3c4

Mythen, G. (2018). Thinking with Ulrich Beck: security, terrorism and transformation. *Journal of Risk Research, 21*(1), 17–28. https://doi.org/10.1080/13669877.2017.1362028

Mythen, G. (2021). The critical theory of world risk society: a retrospective analysis. *Risk Analysis, 41*(3), 533–543. https://doi.org/10.1111/risa.13159

National Whistleblower Center. (2022). *Edward Snowden.* Retrieved 26.03.22, from https://www.whistleblowers.org/whistleblowers/edward-snowden/

Norwegian Food Safety Authority (Mattilsynet). (2022). *Resultater fra radioaktivitetsmålinger på sau og rein høsten 2021.* Retrieved 15.03.22, from https://www.mattilsynet.no/mat_og_vann/uonskede_stofferimaten/radioaktivitet/resultater_fra_radioaktivitetsmaalinger_paa_sau_og_rein_hosten_2021.41459

NSM (Norwegian National Security Authority/Nasjonal sikkerhetsmyndighet). (2015). *Sikkerhetsfaglig råd*. https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/rapporter-og-regelverk/nsm-sikkerhetsfaglig_raad_2015_web.pdf

Ord, T. (2020). *The precipice: existential risk and the future of humanity*. Bloomsbury.

Osterwalder, A. & Pigneur, Y. (2010). *Business model generation: a handbook for visionaries, game changers, and challengers*.

Ovid (2018). *Metamorphoses: the new, annotated edition*. (R. Humphries, Trans.; J. D. Reed, Annotation). Indiana University Press.

Paté-Cornell, M.-E. Kuypers, M., Smith, M. & Keller, P. (2018). Cyber risk management for critical infrastructure: a risk analysis model and three case studies. *Risk Analysis, 38*(2), 226–241. https://doi.org/10.1111/risa.12844

Pentland, B. T. (2016). Risk and routine in the digitized world. In Power, M. (Ed.), *Riskwork* (pp. 193–210). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198753223.003.0010

Peters, G. W., Shevchenko, P. V. & Cohen, R. (2018). Understanding cyber-risk and cyber-insurance. *Macquarie University Faculty of Business & Economics Research Paper*. http://dx.doi.org/10.2139/ssrn.3200166

Pettersen, K. (2016). Understanding uncertainty: thinking through in relation to high-risk technologies. (2016). In Burgess, A., Alemanno, A. & Zinn, J. O. (Eds.), *Routledge handbook of risk studies* (pp. 39–48). Routledge.

Power, M. (2004). *The risk management of everything: rethinking the politics of uncertainty*. Demos. https://www.demos.co.uk/files/riskmanagementofeverything.pdf

Power, M. (2007). *Organized uncertainty: designing a world of risk management*. Oxford University Press.

Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society, 34*(6), 849–855. https://doi.org/10.1016/j.aos.2009.06.001

Proust, M. (1929/2014). *The captive*. Anncona media.

Ramirez, R. & Choucri, N. (2016). Improving interdisciplinary communication with standardized cyber security terminology: a literature review. *IEEE Access*, *4*, 2216–2243. https://doi.org/10.1109/ACCESS.2016.2544381

Rasborg, K. (2021). *Ulrich Beck: theorising world risk society and cosmopolitanism*. Springer. https://doi.org/10.1007/978-3-030-89201-2

Refsdal, A. Solhaug, B. & Stølen, K. (2015). *Cyber-risk management*. Springer. https://doi.org/10.1007/978-3-319-23570-7

Rosa, E. A. (1998). Metatheoretical foundations for post-normal risk. *Journal of risk research, 1*(1), 15–44, https://doi.org/10.1080/136698798377303

Rumsfeld, D. (2010). Author's note. In *Known and unknown*. Retrieved 17.05.22, from https://papers.rumsfeld.com/about/page/authors-note

Røyksund, M. (2011). *Informasjonssikkerhet i kraftforsyningen* [Master thesis]. Universitetet i Stavanger. http://hdl.handle.net/11250/184580

Scala, N. M., Reilly, A. C., Goethals, P. L. & Cukier, M. (2019). Risk and the five hard problems of cybersecurity. *Risk Analysis, 39*(10), 2119–2126. https://doi.org/10.1111/risa.13309

Shelley, M. W. (2020). *Frankenstein*. Saga Egmont. (Original work published 1818)

Silverman, D. (2014). *Interpreting qualitative data* (5th ed.). Sage.

de Smidt, G. & Botzen, W. (2018). Perceptions of corporate cyber risks and insurance decision-making. *Geneva Papers on Risk and Insurance. Issues and Practice, 43*(2), 239–274. https://doi.org/10.1057/s41288-018-0082-7

von Solms, R. & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Society for Risk Analysis. (2018). *Glossary*. https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf

Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, *135*. https://doi.org/10.1016/j.ssci.2020.105143

Strydom, P. (2002). *Risk, environment and society: ongoing debates, current issues and future prospects*. Open University Press.

Sørensen, M. P. (2002). Interview med Ulrich Beck. *Slagmark - Tidsskrift for Idéhistorie,* 34, 125–144.

Sørensen, M. P. (2018). Ulrich Beck: exploring and contesting risk. *Journal of Risk Research, 21*(1), 6–16. https://doi.org/10.1080/13669877.2017.1359204

Themsen, T. N. & Skærbæk, P. (2018). The performativity of risk management frameworks and technologies: the translation of uncertainties into pure and impure risks. *Accounting, Organizations and Society, 67*, 20–33. https://doi.org/10.1016/j.aos.2018.01.001

Tjora, A. (2019). *Qualitative research as stepwise-deductive induction*. Routledge. https://doi.org/10.4324/9780203730072

UNESCO, OECD, IDB (2022). *The effects of AI on the working lives of women*.

Wildavsky, A. (1979). No risk is the highest risk of all. *American scientist, 67*(1), 32–37. https://www.jstor.org/stable/27849058

Willig, C. (2013). *Introducing qualitative research in psychology* (3rd ed.). Open University Press.

World Nuclear Association. (2022). *Chernobyl accident 1986*. Retrieved 15.03.22, from https://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/chernobyl-accident.aspx

DISSERTATION ARTICLES

Article 1: Aakre, S. (2020). "Just tell us what to do" Regulations and cyber risk appetite in the electric power industry. In P. Baraldi, F. Di Maio, & E. Zio (Eds.), *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*. Research Publishing, Singapore.

Article 2: Aakre, S. (2020). Hvilket trusselbilde står norske virksomheter overfor, og hvordan kan åpenhet bidra til å forstå cyberrisiko? *Magma, 20*(2), 18–26.

Article 3: Bourmistrov, A. & Aakre, S. (2020). Framsyn som risikoradar: Hvordan kan scenarioanalyse forbedre cybersikkerhet? *Magma, 20*(2), 55–61.

Article 4: Aakre, S. (2022, preprint). Ransomware as business models.

Article 1: Aakre, S. (2020). "Just tell us what to do" Regulations and cyber risk appetite in the electric power industry. In P. Baraldi, F. Di Maio, & E. Zio (Eds.), *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*. Research Publishing, Singapore.

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

Silje Aakre

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

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

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

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

1. Introduction

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

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

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

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

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

2. Theoretical framework

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

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

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

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

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

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

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

3. Methodology

The data material consists of interviews, observations and documents.

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

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

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

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

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

4. Empirical findings

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

4.1 New regulations

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

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

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

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

4.2 Risk perception and risk acceptance

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

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

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

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

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

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

4.3 Guidance

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

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

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

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

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

5. Concluding discussion

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

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

5.1 Understanding cyber risks

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

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

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

5.2 Rules as legitimacy

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

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

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

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

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

5.3 Who should decide acceptable risk?

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

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

5.4 Closing remark

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

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

Acknowledgement

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

References

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

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

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

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

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

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

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

Article 2: Aakre, S. (2020). Hvilket trusselbilde står norske virksomheter overfor, og hvordan kan åpenhet bidra til å forstå cyberrisiko? *Magma, 20*(2), 18–26.

Hvilket trusselbilde står norske virksomheter overfor, og hvordan kan åpenhet bidra til å forstå cyberrisiko?

SILJE AAKRE er nærings-ph.d.-kandidat i NC-Spectrum AS og tilknyttet handelshøgskolen ved Nord universitet. Hun forsker på cybersikkerhet i kraftbransjen.

SAMMENDRAG

Formålet med artikkelen er å formidle hvilke cybertrusler som dominerer, og hvordan trusselbildet kommuniseres og bør kommuniseres for å gi bedre grunnlag for styring av cyberrisiko. Artikkelen presenterer en definisjon av cyberrisiko og går gjennom aktuelle trusselvurderinger for norske virksomheter. Den anvender teori om kjente og ukjente risikoer og presenterer en modell for hvordan kommunikasjon og åpenhet om risiko kan forstås og bidra til økt situasjonsforståelse. Trusselvurderingene er hentet fra fire myndighetsaktører og to organisasjoner. Analysen viser de mest framtredende cybertruslene og slår fast at cyberrisiko også blir viet betydelig oppmerksomhet i de generelle trusselvurderingene.

INNLEDNING

Samfunnet går fra analogt til digitalt på mange arenaer. Dette gjelder blant annet kjøp og salg av tjenester, offentlig administrasjon, kommunikasjon og kriminalitet. Digitalisering, kunstig intelligens, maskinlæring, smarte løsninger, skytjenester, tingenes internett og stordata skal gi utallige muligheter for økt innovasjon, effektivitet og velferd.

Medaljens bakside er sårbarheter knyttet til teknologi og bruk. Hver gang en ny digital løsning tas i bruk, manifesteres tilhørende risiko. Selv om digitaliseringen kan være en døgnflue, «noe man må skrive om fort, før det blir gammeldags igjen» (Andersen & Sannes, 2017, s. 18), har utfordringene knyttet til cyberrisikoer kommet for å bli. Uønskede cyberhendelser har et bredt spekter og innebærer alt fra nettverksskanninger og datainnbrudd som ikke blir avdekket, til e-post med sensitiv informasjon sendt til feil adresse og omfattende løsepengevirus.

Når «alt skal ha en app» og «alle går over i skyen», følger det med nye sårbarheter og risikoer. Innsamling, lagring, bearbeiding og tilgjengeliggjøring av informasjon er sjelden risikofritt. Da Rema 1000 ønsket å samle og behandle kunders kontaktinformasjon, kjøpsvaner og lokasjon i appen Æ, var det en risiko for at informasjonen kunne komme på avveier. Kort tid etter lanseringen av Æ meldte en forbruker at kundebasen lå åpent tilgjengelig (Gundersen, 2017). Myndigheter og forbrukere forutsetter at sikkerhet er ivaretatt. Dette, kombinert med virksomheters bruk og avhengighet av digitale arbeidsverktøy, kommunikasjonskanaler og tjenester, fordrer at tilhørende cyberrisiko blir en naturlig del av virksomheters risikostyring.

Styring av cyberrisiko kan være krevende fordi risikoene ikke er observerbare og håndfaste som de fleste risikoer i det fysiske rom. Like fullt trengs kompetanse om risiko og kunnskap om trusler for å håndtere risikoen. En forutsetning for å håndtere risiko er informasjon. Gjennomgang av relevant informasjon kan betegnes som første ledd i risikostyring (Aven & Renn, 2010, s. 121). Én lett tilgjengelig kilde til informasjon om cyberrisiko er myndighetenes trusselvurderinger og risikorapporter.

Formålet med artikkelen er å formidle hvilke cybertrusler som dominerer, og hvordan trusselbildet kommuniseres i rapportene. I artikkelen blir det bygget videre på teori om kjente og ukjente risikoer og utviklet en modell for å illustrere hvordan informasjonsutveksling og kommunikasjon kan redusere det ukjente og gi bedre grunnlag for styring av cyberrisiko.

KJENTE OG UKJENTE RISIKOER

Kategoriseringen av hendelser som *kjente kjente, kjente ukjente* eller *ukjente ukjente* ble lagt merke til under en pressekonferanse med USAs daværende forsvarsminister, Donald Rumsfeld, i 2002. Temaet var krigen i Irak. Ordleggingen har fått både pepper og skryt. Han formulerte at det eksisterer kjente kjente – ting vi vet at vi vet. Det eksisterer kjente ukjente – ting vi vet at vi ikke vet. Sist, men ikke minst, eksisterer ukjente ukjente – ting vi ikke vet at vi ikke vet. Det er ifølge Rumsfeld sistnevnte kategori vi bør bekymre oss for (Rumsfeld, 2002). I denne kategorien faller hendelsene vi ofte kaller sorte svaner. Dette er hendelser som er utenkelige for de fleste før de inntreffer, som massakren på Utøya 22. juli 2011. Det har senere blitt argumentert for at ukjente kjente – ting vi ikke vet at vi vet, beskrevet som underbevisstheten – også bør inkluderes (Žižek, 2006, s. 137). De fire kategoriene framstilles ofte som et vindu med fire ruter. Selv om modellen fort ble populær, har flere påpekt utfordringer – blant annet hvorvidt kjente ukjente og ukjente kjente kan eksistere samtidig, eller om den ene leder til den andre (Marshall, Ojiako, Wang, Lin, & Chipulu, 2019, s. 647).

På bakgrunn av dette foreslås en modell (figur 1) som illustrerer hvordan to parter sammen har et bilde av en situasjon, et fenomen, en risiko eller lignende. Modellen skal bidra til å forklare samspillet mellom to parter som har mulighet for informasjonsutveksling. Feltene kan behandles som vinduer hvor vinduets størrelse angir andelen kjent og ukjent kunnskap av totalbildet.

FIGUR 1 Enkel framstilling av kjent og ukjent kunnskap for to parter.

		A	
		Kjent	*Ukjent*
B	*Kjent*	*KJENT (kjent kjent)*	*FORDEKT (ukjent kjent)*
	Ukjent	*FORDEKT (kjent ukjent)*	*UKJENT (ukjent ukjent)*

Informasjonsutveksling kan være ett tiltak for å utvide det kjente vinduets størrelse samtidig som det helt eller delvis ukjente reduseres. Dette bygger på grunntanken om at læring er mulig. Siden partene har ulik kunnskap om totalbildet (feltene for det kjente og ukjente), er problemstillingene knyttet til om alle fire felt kan eksistere samtidig, mindre relevant.

Inkluderingen av hva som er kjent og ukjent for en motpart, kan minne om Joharis vindu. Joharis vindu viser feltene (og trekkene) åpen, skjult, blind og ukjent (Luft & Ingham, 1955, referert i Zahl-Begnum & Begnum, 1990, s. 140). Trekkene beskriver ulike sider ved vår kommunikasjon. Et stort åpent felt vil gi bedre kommunikasjon og mindre sjanse for misforståelse og feiltolkninger. Jo mindre åpne vi er, desto fattigere blir kommunikasjonen, og den stopper gjerne opp etter kort tid (Myrseth, 2013).

Videre i artikkelen benyttes begrepene kjent, fordekt og ukjent, som i figur 1. Fordekt representerer det som er kjent for den ene og ukjent for den andre. Eksempelvis kan en sårbarhet i eget IT-system være kunnskap som er kjent for den ene (A) og ukjent for den andre (B).

UTVALG OG METODE

Datamaterialet består av totalt sju rapporter (tabell 1) som omhandler trusselbilde og risikovurdering. Alle rapportene som analyseres, er ugraderte, gratis og offentlig tilgjengelig.

Norske myndigheter utgir fire trussel- og risikovurderinger årlig. Rapportene utgis av Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST), Direktoratet for samfunnssikkerhet og beredskap (DSB) og Nasjonal sikkerhetsmyndighet (NSM). Vurderingene fra E-tjenesten, PST og NSM utgis årlig. DSB utgir nye krisescenarioer årlig og har så langt utgitt samlerappor-

TABELL 1 Analyserte risiko- og trusselvurderinger.

UTGIVER	REFERANSE	TITTEL	ÅR	SIDETALL
Etterretningstjenesten (E-tjenesten)	(E-tjenesten, 2019)	Fokus 2019	2019	101
Politiets sikkerhetstjeneste (PST)	(PST, 2019)	Trusselvurdering 2019	2019	27
Direktoratet for samfunnssikkerhet og beredskap (DSB)	(DSB, 2019)	Analyser av krisescenarioer 2019	2019	221
Nasjonal sikkerhetsmyndighet (NSM)	(NSM, 2019)	Risiko 2019	2019	32
Norsk senter for informasjonssikring (NorSIS)	(NorSIS, 2018)	Trusler og trender 2018–19	2018	52
Næringslivets sikkerhetsråd (NSR)	(NSR, 2018)	Mørketallsundersøkelsen 2018	2018	63
Næringslivets sikkerhetsråd (NSR)	(NSR, 2019a)	Hybridundersøkelsen	2019	59

ter i 2014 og 2019. I DSBs samlerapport er kun de generelle delene og scenarioer om cybertrusler analysert.

Myndighetenes trusselvurderinger er supplert med tre rapporter fra andre aktører med særskilt satsing på blant annet informasjonssikkerhet og cyberkriminalitet. *Trusler og trender* utgis årlig av Norsk senter for informasjonssikring (NorSIS) og retter seg spesielt mot små og mellomstore virksomheter og privatpersoner. Næringslivets sikkerhetsråd (NSR) har gitt ut to relevante rapporter som bygger på undersøkelser gjennomført i norske virksomheter og bidragsytere som Forsvarets forskningsinstitutt, Visma og Telenor. *Mørketallsundersøkelsen* har blitt utgitt i en årrekke og omhandler temaene informasjonssikkerhet, personvern og datakriminalitet. *Hybridundersøkelsen* ble utgitt for første gang i 2019. Hybride angrep defineres ved at aktørene har et større mål, at flere ulike virkemidler brukes samtidig, og at det er vanskelig å se dem i sammenheng. Eksempler er cyberspionasje, påvirkningsoperasjoner, sabotasje og terrorisme (NSR, 2019a, s. 6). Det er ventet at hybride angrep vil ta i bruk digitale/teknologiske virkemidler. Artikkelen skiller derfor ikke spesielt mellom cyberangrep og hybride angrep utover at det er spesifisert når det snakkes spesifikt om funn fra hybridundersøkelsen.

Det er gjort en kvalitativ innholdsanalyse av alle rapportene. Rapportene er i tillegg gjennomgått for å identifisere cybertrusler som omtales. Cybertruslene fra rapportene er samlet i kategorier av ulike trusler. Kun cybertrusler som er nevnt i flere enn halvparten av rapportene (minimum fire av sju), framgår i tabell 2. Cybertruslene er oppgitt i rekkefølge, med trusselen som er omtalt i flest rapporter, først. Det gis eksempler på trusler fra rapportene i hver kategori.

Videre anvendes modellen i figur 1 for å studere betydningen av åpenhet gjennom hvordan ukjente trusler kan gjøres kjente. Det benyttes eksempler med en myndighetsaktør og en virksomhet inspirert av funn i rapportene. Modellen viser effekten av informasjonsutveksling mellom to parter.

HVA ER CYBERRISIKO, OG HVILKE CYBERTRUSLER ER DE MEST FRAMTREDENDE?

Trusselvurderingene benytter ulike begreper for cyberrisiko og cybertrusler. Begreper som digital, IKT og cyber har nyanseforskjeller, men blir ofte behandlet som synonymer. Både nasjonalt og internasjonalt blir begrepet cybersikkerhet stadig oftere brukt. På bakgrunn av dette anbefaler NSM (2015, s. 11, 25, 40) at begrepet cybersikkerhet bør erstatte IKT-sikkerhet og benyttes i politiske og strategiske dokumenter. Videre i denne artikkelen benyttes primært prefikset cyber- for trusler og risikoer som blir drøftet.

Det finnes få formelle definisjoner på cyberrisiko. Cyber kan forklares som «det som er relatert til datamaskiner, IKT og nettverk, både digital informasjon og fysiske objekter» (Norsk utenrikspolitisk institutt, 2019). Det er ikke enighet om én definisjon av risiko, men flere vektlegger ventet tap eller skade på verdier, eventuelt sannsynligheten for skade hvor usikkerhet er involvert. Denne artikkelen benytter følgende definisjon: *Cyberrisiko er verdier satt på spill gjennom digitalisering. Verdiene kan være både materielle og immaterielle, og risikoen kan oppstå både tilsiktet og utilsiktet.*

Gjennom digitaliseringen har kjente former for risiko tatt skrittet over i cyberdomenet, som svindel og informasjonstyveri. Vi åpner også for nye risikoer

TABELL 2 De mest framtredende cybertruslene.

CYBERTRUSSEL	EKSEMPEL
Nettverksoperasjoner	Nettverksangrep, hacking
Kompromitteringer	Informasjonslekkasje, overvåking av e-postkorrespondanse, kompromittering f.eks. via utdaterte webservere, adgangssystem på internett, minnepinner
Kartlegging	Skanninger (ofte automatiserte) for å lete etter sårbarheter, kartlegging av ansattes e-poster, rolle og funksjon i virksomheten, brukerprofiler i sosiale medier, innsamling av data gjennom falske henvendelser
Svindel	Nettfiske (*phishing*), direktørsvindel, fakturasvindel, investeringssvindel
Etterretning fra fremmede stater	Rekruttering og føring av hemmelige kilder, nettverksbaserte etterretningsoperasjoner, plassering av studenter og forskere
Skadevare	Virus- og skadevareinfeksjoner, e-post med infiserte vedlegg eller lenke til «vannhull» (nettside med skadevare)
Sabotasje	Skader på maskin- og programvare, sletting av informasjon, endring av konfigurasjon på system, *defacing* (vandalisme mot en nettsides utseende og/eller innhold)
Spionasje	Industrispionasje, digital spionasje
Utnytte sårbarheter	Utnytte kjente sårbarheter, utnytte nulldagssårbarheter (ikke kjente), utnytte sårbarheter i digital infrastruktur og verdikjeder
Løsepengevirus	Krypteringsvirus for økonomisk utpressing, kryptolåsing
Tjenestenektangrep	DDoS-angrep, trusler om DDoS-angrep, overbelaste systemer
Misbruk av ressurser	Graving etter kryptovaluta, *kryptojacking*, misbruk av ressurser til nye angrep, utnyttelse av tredjeparts infrastruktur
Påvirkningsoperasjoner	Påvirkningsforsøk og informasjonskampanjer, falske nyheter, innhentingsoperasjoner og forsøk på påvirkning
Innsidere	Utro tjenere, kan være plassert, utsatt for press eller operere på eget initiativ

ved å koble utstyr til internett. Et akvarium koblet til internett for å overvåke fôring, temperatur og renhold, ble misbrukt som veien inn i et amerikansk kasino for å stjele data (Schiffer, 2017). Dagbladet publiserte i 2013 en rekke artikler i serien «null ctrl» som avdekket alt fra private videokameraer til sensitiv kundeinformasjon og alarmsystemer som lå åpent på nett. Problematikken er med andre ord verken ny eller utdatert.

Sammenkobling av teknologi, aktører og systemer i lange verdikjeder øker risikoen for at virksomheter mister kontrollen på hvor verdifull informasjon er lagret, og hvem som eventuelt har tilgang til den (NorSIS, 2018s. 35). Selv myndighetene vedgår at det nærmest er umulig å holde oversikt over avhengigheter og sårbarheter i en uoversiktlig og kompleks digital infrastruktur (NSM, 2019, s. 15).

NSM NorCERT registrerte i 2018 cirka 20 000 saker der kun nær en fjerdedel ble undersøkt nærmere (NSM, 2019, s. 10). Visma beskriver enkelte typer cyberangrep som så vanlige at de anses som «normal bakgrunnsstøy» fordi de foregår i stort omfang. Det henvises her primært til automatiserte skanninger. Beregninger viser at angrep og angrepsforsøk mot de tjenestene Visma leverer, ville gitt grunnlag for 1 800–3 000 anmeldelser i måneden (NSR, 2018, s. 51).

Av datamaterialet framgår det tydelig at cybertrusler er noe virksomheter må forholde seg til. Alle myndighetsaktørene har bredere ansvarsområder enn cybersikkerhet. Likevel preger cybertrusler og -risikoer samtlige av rapportene. Dette gjelder både som definerte utfordringsområder og som verktøy eller virkemidler i andre trusler.

Gjennomgangen av rapportene identifiserte 177 cybertrusler. Enkelte cybertrusler går igjen i flere av rapportene, men er kun registrert én gang per rapport. Truslene er deretter kategorisert. Tabell 2 viser de 14 mest framtredende cybertruslene fra de sju analyserte rapportene. Kolonnen for eksempler viser noen av cybertruslene som ligger innunder kategorien.

Enkelte cybertrusler er ikke nødvendigvis ulovlige, men ofte i en gråsone fordi aktivitetene gjerne brukes som ledd i et framtidig cyberangrep. Ett eksempel på dette er skanninger. Visma illustrerer skanninger i Mørketallsundersøkelsen med at en ukjent person tester utgangsdører for å se om de er åpne eller låst (Visma i NSR, 2018, s. 51).

Angrep benytter gjerne flere virkemidler i kombinasjon. For eksempel kan en trusselaktør bruke tid på å skanne nettverket og kartlegge bedriftens ansatte og relasjoner. Informasjonen kan brukes til å iverksette mer målrettet nettfiske for å manipulere til handling. Målet kan være å kryptere virksomhetens filer for å kreve løsepenger.

Det rapporteres også om tilpasset svindel. Tilpasset svindel kan være falske e-poster fra en tjeneste du har et kundeforhold til, eller sesongbasert, som «henting av pakke» i desember. Selv utpressingsbeløp kan være tilpasset. I praksis betyr det at virksomheter blir presset for høyere beløp enn privatpersoner (NorSIS, 2018, s. 36–37).

Det er krevende å skille mellom eller finne ut av om angrep er økonomisk kriminalitet, statlige angrep, uhell og feil eller «jente- og guttestreker» (NSR, 2019a, s. 44). I det praktiske arbeidet spiller kanskje dette uansett mindre rolle. Hovedforskjellen antas å være at statlige aktører har «ubegrenset» med ressurser og tid, mens vinningskriminelle vil gå over til andre mål dersom virksomheten er «sikker nok».

HVORDAN KOMMUNISERER AKTØRENE TRUSSELBILDET OG TILTAK?

Flere av aktørene legger fram et trusselbilde som karakteriseres av endring. Noen beskrivelser er «sammensatt og i rask endring og utvikling» (E-tjenesten, 2019, s. 9), «dynamisk» (NSM, 2019, s. 5) og «i kontinuerlig endring» (DSB, 2019, s. 9). Dette er stikk i strid med PSTs (2019, s. 3) vurdering «stabile og relativt varige utviklingstrekk». NorSIS (2018, s. 29) rapporterer også at årets trusler ikke divergerer stort fra året før. NorSIS peker i tillegg på en nyanse her: Selv om metodene er de samme som tidligere, oppfattes trusselaktørene og angrepene som mer avanserte og målrettede.

Ulike vurderinger av risikobildet kan også skyldes at myndighetene har ulike instrukser og mandat. Likevel kan de tidvis vage beskrivelsene av trusselbildet føre til at nytten av rapportene går ned. Informasjonen kan oppleves som intetsigende og lite pålitelig når det gis motstridende vurderinger. Av virksomhetene oppgir kun 17 prosent å ha lest PSTs risikovurdering og kun 10 prosent å ha lest NSMs risikovurdering (NSR, 2019b, s. 16). Dette kan indikere at rapportene ikke blir oppfattet som relevante for virksomhetene. Dersom myndighetene ønsker å være primærkilden for norske virksomheter i framtiden, må det gis informasjon som virksomhetene faktisk forstår og kan bruke i risikostyringsarbeidet.

Mange trenger hjelp til å omsette kunnskap i tiltak (NSR, 2018, s. 61). Rapportene viser en rekke punkter hvor sikkerheten bør bedres, men gir få konkrete tiltak. Eksempelvis anbefales det å arbeide med «sikkerhetsstyring», «risikovurderinger» og å «redusere sårbarheter» uten at det nødvendigvis gis gode svar på hvordan dette kan gjøres. E-tjenestens trusselvurdering skiller seg ut ved å ikke anbefale ett eneste tiltak for å redusere risiko. PST, NSM og DSB kommer med anbefalte tiltak, men er ikke i nærheten av å være like grundige som NorSIS og NSR. Her bør det nevnes at særlig NSM har gitt ut en rekke veiledninger og temarapporter i tillegg til den årlige trusselvurderingen. Eksempler er *Grunnprinsipper for IKT-sikkerhet* og *Håndtering av digital spionasje*. Begge presenterer en rekke tiltak.

ÅPENHET ER INTENSJONEN, MEN IKKE PRAKSISEN?

Økt åpenhet kan bidra til at angrep blir avverget. Når færre angrep lykkes, blir cyberangrep en mindre lønnsom forretningsmodell. På sikt kan dette kanskje gi færre angrep. I rapportene er det bred enighet om at samarbeid, åpenhet og informasjonsutveksling er nødvendig for å møte cybertruslene (NSR, 2018, s. 50, 2019a, s. 44; NSM, 2019, s. 50; NorSIS, 2018, s. 41).

Den nye sikkerhetsloven (i kraft fra 01.01.19) legger opp til bedre samhandling og mer informasjonsdeling mellom myndigheter og virksomheter som er underlagt loven. Det pekes på at myndighetene også har behov for mer innrapportering av hendelser (NSM, 2019, s. 25). Selv om svært få rapporterer og anmelder hendelser, svarer hele 92 prosent av virksomhetene at de ønsker å dele informasjon med myndighetene (NSR, 2019a, s. 39).

Hybridundersøkelsen understreker at økt åpenhet fra myndighetene er ønsket. Over halvparten svarer at de mener norske myndigheter bør bidra med mer informasjon, klarere retningslinjer, veiledning og åpenhet om hybride hendelser som myndighetene vet om (NSR, 2019a, s. 29).

Rapportene viser derimot manglende åpenhet som går begge veier. Av virksomheter som opplevde sikkerhetshendelser, rapporterte kun ni prosent til politiet, og fem, tre og to prosent til andre myndighetsaktører, Nor-CERT eller sektor-CERT og lignende. Det vanligste er å rapportere til administratoren av det aktuelle systemet

(72 prosent). En del melder også til antivirusleverandør (24 prosent) og ISP (internettleverandør) (10 prosent). (NSR, 2018, s. 28) En av grunnene til at få anmelder, kan være manglende bevissthet rundt hva som er en kriminell handling. Det råder også en oppfatning om at en anmeldelse vil gi merarbeid for virksomheten, og at politiet ikke har ressurser til å følge opp (NSR, 2018, s. 50). Med Vismas beregninger av grunnlag for 1 800–3 000 anmeldelser i måneden er det klart at dette vil gi betydelig merarbeid – og mange henleggelser.

Noen virksomheter ønsker ikke at kunder, leverandører og konkurrenter skal få vite om eventuelle hendelser. Dette fører til at de dysses ned (NorSIS, 2018, s. 30). Årsakene kan være at virksomheten ikke ønsker å framstå som et enkelt mål eller svekke tilliten i aksjemarkedet (NSR, 2019a, s. 44). Sikkerhetshendelser kan også virke stigmatiserende dersom allmennoppfatningen er at virksomheten burde gjort mer for å unngå hendelsen (NorSIS, 2018, s. 29). I utpressingssaker oppfatter ofrene det ofte som mer attraktivt å betale enn å søke hjelp eller melde fra (NorSIS, 2018, s. 29). Dette kan gi uheldige ringvirkninger. Det viser at virksomheten er et mulig offer for framtidige angrep. I løsepengevirussaker er det ingen garanti for at filer blir dekryptert, eller at aktøren ikke har installert en bakdør for framtidige angrep. I tillegg bidrar løsepenger til å opprettholde den kriminelle forretningsmodellen.

I trusselvurderingens innledning skiver sjef for E-tjenesten at det er utfordrende å ikke kunne dele gradert informasjon. Som en følge vil enkelte områder ikke være dekket av trusselvurderingen (E-tjenesten, 2019, s. 6). Det kan spørres om det alltid er forsvarlig å være åpen om sårbarheter og angrep. Informasjonen kan i verste fall forstås som en oppskrift til vinningskriminelle og etterretning. Funn som at «ved sikkerhetsbrudd har industri-, overnattings- og serveringsvirksomheter samt tjenesteytende næringer lavest modenhet for oppdagelse» (NSR, 2018, s. 37), gir en pekepinn om i hvilke bransjer det kan være større sjanse for å lykkes med cyberangrep.

DILEMMAET TAUSHET ELLER ÅPENHET – TO EKSEMPLER

Equifax-skandalen illustrerer både den økonomiske konsekvensen og stigmatiseringen som et cyberangrep kan føre til. I 2017 ble det kjent at personopplysninger som kredittovervåkingsbyrået Equifax lagret, var på avveier. Denne typen informasjon kan misbrukes til blant annet identitetstyveri. Datalekkasjen rammet over 146 millioner individer, primært amerikanere (U.S. Government Accountability Office, 2018, s. 1). I løpet av dager falt aksjeverdien med en tredjedel (MarketWatch, 2019). I 2019 ble det besluttet at Equifax må betale opptil 700 millioner dollar i oppgjør etter hendelsen (Schroeder, 2019). I ettertid har det kommet fram at Equifax hadde sårbarheter som kunne vært eliminert eller redusert. Oppdatering av programvaren ville tettet sikkerhetshullet som ble utnyttet. Databasene var ikke segmentert (isolert), slik at angriperne lettere fikk tak i mer informasjon. Angriperne fikk tilgang til databaser hvor brukernavn og passord lå ukryptert. Det var heller ikke tak på antall spørringer som kunne gjøres mot databasen. (U.S. Government Accountability Office, 2018, s. 15–16)

En aktør som håndterte en cyberhendelse ganske annerledes enn Equifax, er Hydro. Når denne artikkelen trykkes, er det cirka ett år siden nyheten kom om at Hydro var utsatt for et omfattende cyberangrep. Selve inntrengningen skjedde ved at et vedlegg i en e-post fra en kunde til en ansatt i Hydro ble kapret og utstyrt med skadevare. Vedlegget var del av en reell og ventet korrespondanse i legitim kommunikasjon i en kunderelasjon (Briggs, 2020). Skadevaren var fordekt som en legitim fil, altså en trojansk hest. Dette skjedde tre–fire måneder før selve angrepet. I denne perioden arbeidet angriperen(e) med å skaffe tilganger for å gjennomføre angrepet (Moberg & Lekanger, 2019). Da krypteringen av servere og datamaskiner begynte, var Hydro tidlig ute med pressekonferanse, anmeldelse og informasjon til media. For dette mottok Hydro Kommunikasjonsforeningens åpenhetspris 2019 (Mellum, 2019).

I ettertid har det blitt kjent at Hydros åpenhet, og særlig bevismaterialet som ble delt med myndighetene, var nyttige for andre formål enn kun etterforskning. Ved hjelp av bevismaterialet kunne det spores opp angrep med samme virus fra de samme hackerne på et tidlig stadium. Dette gjorde det mulig å varsle virksomhetene og avverge angrep. Flere norske og utenlandske virksomheter var blant de utsatte. (Klevstrand, 2019)

De færreste av oss er i særlig grad selvforsynte, verken privat, på virksomhetsnivå eller på samfunnsnivå. Istedenfor benyttes kjøp av varer og tjenester – også innen cyber. Dette skaper et avhengighetsforhold hvor sårbarheter og cyberangrep hos én virksomhet, én person eller ett system kan få følgehendelser og konsekvenser for flere i verdikjeden. Angrepet mot Hydro

var ikke en IT-krise, men en virksomhetskrise som fikk store konsekvenser for hele driften – fra aluminiumsproduksjon til utbetalinger av lønn.

Tiltak koster, i det minste i tid: Det er knappe ressurser, og det må prioriteres. NorSIS (2018, s. 31) antar at mange virksomheter iverksetter tiltak først *etter* hendelser. I slike tilfeller sitter virksomheten med kostnaden både for tapt inntekt under angrepet, opprydningsarbeid og investeringer i sikkerhet. Kostnadene kunne derimot vært langt lavere, kanskje til og med avverget hendelsen, om de ble gjort tidligere. Hydro (2019) anslår selv at cyberangrepet som rammet dem, kostet 550–650 millioner kroner. Kostnader for virksomheter flest er ifølge Mørketallsundersøkelsen i snitt drøyt 54 000 kroner for den mest alvorlige hendelsen. De som er hardest rammet, estimerer en kostnad på to millioner kroner. Merk at tallene inkluderer de som oppgir at hendelsen ikke har hatt noen kostnad. (NSR, 2018, s. 28)

HVORDAN GJØRE UKJENTE RISIKOER KJENTE?

Modellen som ble introdusert innledningsvis (figur 1), er benyttet for å illustrere to parters kunnskap om trusselbildet (figur 2). Eksempler på informasjon i figuren er hentet fra analysen av rapportene. Både virksomheten og myndighetsaktøren kjenner til hendelser som blir delt, og de åpne trusselvurderingene. Videre har virksomheten kunnskap om angrep som ikke er rapportert, og som myndighetsaktøren derfor ikke kjenner til. Myndighetsaktøren har på sin side kunnskap om gradert informasjon og hendelser som ikke er delt i åpne kilder. Partene deler et ukjent felt, for eksempel kartleggingsangrep som ingen av dem har oppdaget.

Feltene som er kjent for den ene parten, men ukjent for den andre, utgjør et potensial for informasjonsutveksling og økt kunnskap. Dersom myndighetsaktøren eksempelvis deler informasjon utover den offentlige trusselvurderingen, vil virksomhetens kjente felt øke. Dette er illustrert i figur 3. Myndighetsaktøren har i dette eksempelet ingen endring i sin andel av kunnskap som er kjent eller ukjent. Figur 4 illustrerer endring i myndighetsaktørens kjente felt som resultat av informasjonsdeling fra virksomheten.

Når myndighetsaktøren deler informasjon, øker virksomhetens kjente felt, og vice versa. Som resultat blir andelen kjent og felles kunnskap større.

FIGUR 2 Eksempler på kjent og ukjent informasjon om cyberrisiko for en virksomheten og en myndighetsaktør.

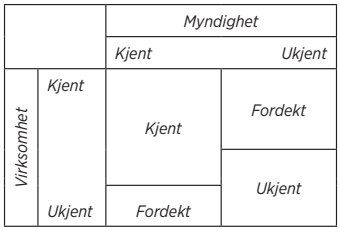
		Myndighet	
		Kjent	*Ukjent*
Virksomhet	*Kjent*	*Hendelser som blir delt, åpne trusselvurderinger*	*Angrep som ikke blir registrert eller anmeldt*
	Ukjent	*Gradert trusselvurdering, det som ikke deles i trusselvurderingene*	*Risiko/angrep ingen av aktørene er klar over, f.eks. kartleggingsangrep*

Figur 5 illustrerer antatt effekt dersom begge partene deler informasjon med hverandre. Her har det kjente feltet også økt på bekostning av det ukjente feltet. Dette baseres på at det å se informasjon i sammenheng kan gi grunnlag for å trekke nye slutninger og gi ny kunnskap. Et eksempel som er beslektet med artikkelens tema, er Cambridge Analyticas bearbeiding av informasjon. De benyttet informasjon fra Facebook-profiler til å finne korrelasjoner mellom liker-klikk og karaktertrekk. Dette muliggjorde at de på bakgrunn av lite informasjon om en enkeltperson kunne danne seg et større og treffsikkert bilde av individets personlighetstrekk og dermed interesser, preferanser og politiske ståsted (NSR, 2019a, s. 46–47). Ved hjelp av stordata kunne et liker-klikk til «Hello Kitty» på Facebook gi sterke indikasjoner om et individs politiske ståsted (Cadwalladr & Graham-Harrison, 2018).

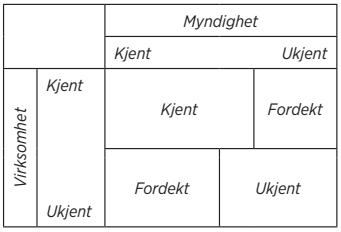
Modellen illustrerer hvordan informasjonsutveksling og ny kunnskap kan minimere feltene som er helt eller delvis ukjente. I hvor stor grad dette kan oppnås, avhenger blant annet av partenes kunnskap om situasjonen og kvaliteten på kommunikasjonen. Det kan være utopisk å anta at hele situasjonsbildet kan gjøres kjent. Målet bør heller være å benytte informasjonsdeling for å redusere de helt eller delvis ukjente feltene så langt det lar seg gjøre, og der dette er til alles fordel. Informasjonsutveksling kan dessuten betraktes som «lavthengende frukt» både organisatorisk og kostnadsmessig.

Åpenhet er ikke synonymt med førstesideoppslag i alle landets aviser. Det bør ved ulike hendelser avgjøres hvilken grad av åpenhet som er konstruktiv. Alternativer omfatter rapportering til myndighetene, inkludert lovpålagt rapportering; deling i lukkede fora som bransjefora og sektor-CERT; informasjon til berørte parter

FIGUR 3 Resultat av informasjonsdeling fra myndighetsaktør til virksomhet illustrert ved endring i vinduenes størrelse.



FIGUR 4 Resultat av informasjonsdeling fra virksomhet til myndighetsaktør illustrert ved endring i vinduenes størrelse.



(kunder, leverandører, samarbeidspartnere, ansatte); eller åpen deling på nettside, i media eller lignende.

Rapportene viser at både virksomheter og myndighetene har forbedringspotensial innen informasjonsdeling. Det bør vurderes om det er behov for å tilpasse eksisterende rapportering, kanaler eller fora for å dele. Videre er det viktig å unngå stigmatisering som kan hemme åpenhet. Mediene har ofte skarpt søkelys på person og virksomhet, noe som kan være belastende for dem som befinner seg i en allerede krevende hendelse. Basert på Hydro-saken kan det se ut til at virksomheter kan unngå spekulerende og negativ omtale ved å informere om en cyberhendelse selv.

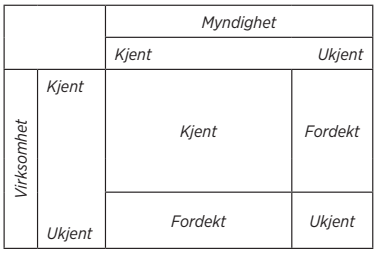
Modellen er, i likhet med alle andre modeller, en forenkling. I praksis er vi omgitt av flere aktører og situasjoner vi har svært ulikt kunnskapsnivå rundt. I tillegg kan kunnskapen vi har, være usikker. Likevel viser modellen hvordan åpenhet kan bidra til at ukjente risikoer gjøres kjente. Når alle deler, blir ukjent kjent. Både myndighetene og virksomhetene etterlyser mer informasjonsutveksling. Dette tyder på at det er et stort potensial for økt kunnskap gjennom informasjonsutveksling.

KONKLUSJON

Kunnskap om trusler og risiko er grunnleggende for risikostyringen. Datagrunnlaget er basert på sju rapporter om risikovurderinger og trusselbilde. Cyberrisiko defineres som verdier satt på spill gjennom digitalisering. Ut fra rapportene identifiseres 14 cybertrusler som de mest framtredende. Det vises også at organisasjonene, i større grad enn myndighetene, bistår med konkrete tiltak for styring av cyberrisiko i trusselvurderingene.

Åpenhet er et gjennomgående tema i innholdsanalysen av rapportene. Både myndighetene og virksomhetene er enige om at informasjonsutveksling og åpenhet er

FIGUR 5 Effekt av informasjonsdeling fra og til begge aktørene.



ønskelig og nødvendig for å møte cybertrusler. På tross av dette er noen av rapportene preget av tidvis vage formuleringer om trusler og tiltak. Informasjonen som deles, er i noen tilfeller begrenset. Fra virksomhetenes side vises det at svært få varsler eller anmelder cyberangrep, til tross for at de ønsker mer informasjon og åpenhet. I noen tilfeller ønsker virksomhetene å dysse ned hendelser fordi det kan gi store konsekvenser for økonomi og omdømme og føre til stigmatisering og merarbeid om hendelsen blir kjent (slik som i Equifax' tilfelle). På den andre siden ser vi at informasjonsdeling og åpenhet, spesielt på et tidlig stadium, kan bidra til å avdekke og avverge ytterligere angrep (slik som i Hydro-saken).

Denne artikkelen har presentert en modell for kjent og ukjent kunnskap. Modellen belyser hvordan to parter kan utveksle informasjon. Informasjonsutvekslingen kan øke andelen kjent kunnskap og minimere helt eller delvis ukjent kunnskap. Dette gjelder også ved at sammenstilling av informasjon kan bidra til å danne ny kunnskap som tidligere var ukjent for begge parter. Åpenhet er sentralt for å realisere informasjonsutveksling, oppnå kunnskap og gjøre ukjente risikoer kjente. M

REFERANSER

Andersen, E., & Sannes, R. (2017). Hva er digitalisering? *Magma, 20*(6), 18–24. Hentet fra https://www.magma.no/hva-er-digitalisering

Aven, T., & Renn, O. (2010). *Risk management and governance: Concepts, guidelines and applications*. I J.L. Mumpower & O. Renn (Red.), *Risk, governance and society. Volum 16*. Berlin, Heidelberg: Springer.

Briggs, B. (2019, 16. desember). Hackers hit Norsk Hydro with ransomware. The company responded with transparency. *Microsoft Transform*. Hentet 31.01.2020 fra https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

Cadwalladr, C., & Graham-Harrison, E. (2018, 17. mars). How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool. *The Guardian*. Hentet 02.02.2020 fra https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm

Direktoratet for samfunnssikkerhet og beredskap. (2019). *Analyser av krisescenarioer 2019*. Hentet 05.08.2019 fra https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf

Etterretningstjenesten. (2019). *FOKUS 2019*. Hentet 15.08.2019 fra https://forsvaret.no/fakta_/ForsvaretDocuments/fokus2019_web.pdf

Gundersen, I. (2017, 2. februar). Kundeinfo lå åpent i Rema 1000s Æ-app. *Stavanger Aftenblad*, s. 12.

Hydro. (2019). Cyberangrep på Hydro. Hentet 12.02.2020 fra https://www.hydro.com/no-NO/media/pa-dagsorden/cyberangrep-pa-hydro/

Klevstrand, A. (2019, 8. september). Stoppet hackerangrep mot flere norske selskaper. *Dagens Næringsliv*. Hentet 15.11.2019 fra https://www.dn.no/bors/hydro/datasikkerhet/hacking/stoppet-hackerangrep-mot-flere-norske-selskaper/2-1-666418

MarketWatch. (2019). Equifax Inc. Hentet 24.10.2019 fra https://www.marketwatch.com/investing/stock/efx/charts

Marshall, A., Ojiako, U., Wang, V., Lin, F., & Chipulu, M. (2019). Forecasting unknown-unknowns by boosting the risk radar within the risk intelligent organisation. *International Journal of Forecasting*, *35*(2), 644–658. https://doi.org/10.1016/j.ijforecast.2018.07.015

Mellum, M. (2019). Kommunikasjonsforeningens Åpenhetspris 2019 til Hydro. Hentet 28.10.2019 fra https://www.kommunikasjon.no/fagstoff/nyheter/kommunikasjonsforeningens-apenhetspris-2019-til-hydro

Moberg, J. M., & Lekanger, K. (2019, 5. november). Offer for omfattende dataangrep – slik kan næringslivet ta forholdsregler. *Digi.no*. Hentet 05.11.2019 fra https://www.digi.no/artikler/intervju-offer-for-omfattende-dataangrep-slik-kan-naeringslivet-ta-forholdsregler/477063

Myrseth, H. (2013). Joharis vindu. Hentet 15.11.2019 fra https://ndla.no/subjects/subject:18/topic:1:193544/topic:1:82776/resource:1:116760

Næringslivets sikkerhetsråd. (2018). *Mørketallsundersøkelsen 2018: Informasjonssikkerhet, personvern og datakriminalitet*. Hentet 22.10.2019 fra https://www.nsr-org.no/getfile.php/1311303-1537281687/Bilder/Mørketallsundersøkelsen/Mørketallsundersøkelsen 2018 low.pdf

Næringslivets sikkerhetsråd. (2019a). *Hybridundersøkelsen: Hybride trusler og hendelser mot norsk næringsliv*. Hentet 19.08.2019 fra https://www.nsr-org.no/getfile.php/1312167-1553166117/Dokumenter/NSR publikasjoner/Hybridundersøkelsen/Hybridundersøkelsen_web.pdf

Næringslivets sikkerhetsråd. (2019b). *Kriminalitets- og sikkerhetsundersøkelsen i Norge (KRISINO) 2019*. Hentet 06.11.2019 fra https://www.nsr-org.no/getfile.php/1312949-1568794843/Bilder/Krisino/KRISINO rapport 2019 low.pdf

Nasjonal sikkerhetsmyndighet. (2015). *Sikkerhetsfaglig råd*. Hentet 05.11.2019 fra https://www.nsm.stat.no/globalassets/rapporter/nsm-sikkerhetsfaglig_raad_2015_web.pdf

Nasjonal sikkerhetsmyndighet. (2019). *RISIKO 2019 Krafttak for et sikrere Norge*. Hentet 23.08.2019 fra https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf

Norsk senter for informasjonssikring. (2018). *Trusler og trender 2018–19: Hvilke digitale trusler møter oss på jobb og i hverdagen?* Hentet 15.08.2019 fra http://norsis.no/upload/trusler og trender 2018–19 web.pdf

Norsk utenrikspolitisk institutt. (2019). Cyber. Hentet 27.10.2019 fra https://www.nupi.no/Vaar-forskning/Temaer/Forsvar-og-sikkerhet/Cyber

Politiets sikkerhetstjeneste. (2019). *Trusselvurdering 2019*. Hentet 15.08.2019 fra https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2019.pdf

Rumsfeld, D. (2002, 12. februar). DoD News Briefing – Secretary Rumsfeld and Gen. Myers. Hentet 24.10.2019 fra https://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636

Schiffer, A. (2017, 21. juli). How a fish tank helped hack a casino. *The Washington Post*. Hentet 25.10.2019 fra https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

Schroeder, P. (2019, 22. juli). Equifax's $700 million data breach settlement spurs criticism, calls for new rules. *Reuters*. Hentet 25.10.2019 fra https://www.reuters.com/article/us-equifax-cyber-settlement/equifax-to-pay-up-to-650-million-in-data-breach-settlement-idUSKCN1UH16Y?feedType=RSS&feedName=technologyNews

U.S. Government Accountability Office. (2018). *DATA PROTECTION: Actions taken by Equifax and federal agencies in response to the 2017 breach. GAO-18-559*. Hentet 24.10.2019 fra https://www.gao.gov/assets/700/694158.pdf

Zahl-Begnum, O.H., & Begnum, S. (1990). *Arbeids- og organisasjonspsykologi* (2. utgave). Oslo: NKS-forlaget.

Žižek, S. (2006). Philosophy, the «unknown knowns,» and the public use of reason. *Topoi*, *25*(1–2), 137–142. https://doi.org/10.1007/s11245-006-0021-2

Article 3: Bourmistrov, A. & Aakre, S. (2020). Framsyn som risikoradar: Hvordan kan scenarioanalyse forbedre cybersikkerhet? *Magma, 20*(2), 55–61.

Framsyn som risikoradar

Hvordan kan scenarioanalyse forbedre cybersikkerhet?

ANATOLI BOURMISTROV er professor ved handelshøgskolen, Nord universitet og forskerkoordinator ved Nordområdesenteret. Han har mastergrad i romfartsteknologi Baltisk State Technical University, er siviløkonom fra Bodø, og har doktorgrad fra NHH. Hans forskningsinteresser ligger i fagområdene regnskap, økonomistyring, scenariometoder, økonomisk informasjon og mentale modeller.

SILJE AAKRE er nærings-ph.d.-kandidat i NC-Spectrum AS og tilknyttet handelshøgskolen ved Nord universitet. Hun forsker på cybersikkerhet i kraftbransjen.

SAMMENDRAG

Økt digitalisering og følgelig økt kompleksitet i samspillet mellom teknologi og mennesker skaper nye cybertrusler og øker sårbarhetsflaten for alle typer virksomheter. Tradisjonelle risikostyringssystemer er ikke lenger tilstrekkelig fordi de er reaktive, primært avdekker hendelser etter de har skjedd, og bygger på analyser av tidligere uønskede hendelser som sier lite om nye potensielle trusler. Utfordringen er hvordan en virksomhet kan tilegne seg ny kunnskap som gjør det mulig å forebygge hendelser før de inntreffer.

Denne artikkelen gir en konseptuell diskusjon av hvordan framsyn i form av scenarioanalyse kan forbedre cybersikkerheten og redusere organisatorisk sårbarhet. Vi analyserer litteratur innen fagområdene risikostyring, cyberrisiko og framsyn og diskuterer hvordan scenarioanalyser kan brukes av virksomheter for å løfte kunnskapen om potensielle trusler og øke beredskapen. Vi viser at framsyn kan motvirke en illusjon om kontroll som oppstår når tradisjonell, reaktiv risikostyring anvendes til å håndtere usikkerhet og såkalte sorte svaner. Scenarioanalyse utgjør en organisatorisk intervensjon som er ment å skape en arena for kunnskapsdeling mellom ulike aktører både innenfor og utenfor virksomheten. Scenarioer kan ses på som en risikoradar, blant annet gjennom å tilrettelegge for forebyggende og proaktive holdninger til metoder for risikostyring. Artikkelen konkluderer med at framsyn også kan bringe potensielle dilemmaer og fallgruver inn i virksomheter gjennom organisatorisk grensearbeid, selvoppfyllende profetier og trekk av en paranoid organisasjon.

INNLEDNING

Norske virksomheter møter i økende grad nye, innovative typer cybertrusler. Som motsvar benyttes både helhetlige risikostyringssystemer, internkontrollsystemer og overvåking av nettverkstrafikk i varierende omfang. Samtidig ser vi at mange virksomheter som benytter formelle systemer, fortsatt kan være sårbare. Dette er fordi styringsfunksjonen primært brukes til å avdekke hendelser etter at de har inntruffet, men ikke til å forebygge hendelser (Kulset & Meidelsen, 2020, s. 54). I likhet med dette baserer de fleste inntrengningsdeteksjonssystemene (IDS) seg på å varsle om

uønsket trafikk som allerede har blitt registrert i nettverket. Videre er hva som varsles om, typisk basert på historiske data om allerede kjente trusler.

En generell kritikk i litteraturen (Leitch, 2008, s. xiii) er at risikostyring i beste fall oppfattes som reaktiv og i verste fall bærer preg av sjekklister og pliktarbeid med liten effekt. Tradisjonell risikostyring basert på historiske data er ofte uegnet til å håndtere økende kompleksitet og usikkerhet med hensyn til potensielle trusler. God oversikt og kunnskap om cyberhendelser som har skjedd tidligere, garanterer ikke at virksomheter er godt forberedt på å håndtere andre typer cyberhendelser i framtiden. Risikostyringen bør bidra til bedret beredskap mot nye og ukjente typer cybertrusler. Ved å kun fokusere på avdekking er ikke virksomhetene proaktive i risikostyringen. Som følge kan risikoen for å bli rammet av nye, uønskede hendelser øke. På virksomhetsnivå kan en hendelse medføre blant annet tap av omdømme og økonomiske tap i form av bøter, skade på utstyr og tapt inntekt. På samfunnsnivå kan tilfeller hvor kritisk infrastruktur er rammet av cyberangrep, medføre fare for liv, helse og samfunnssikkerheten.

En mer proaktiv tilnærming til risikostyring er nødvendig for å møte trusler hvor menneskelige faktorer er involvert (Marshall, Ojiako, Wang, Lin, & Chipulu, 2019, s. 645). Nøkkelspørsmålet er: Hvordan kan virksomheter tilrettelegge for mer proaktiv og forebyggende risikostyring som også kan angi potensielle framtidige og foreløpig ukjente cybertrusler? Formålet med denne artikkelen er å diskutere konseptuelt hvordan framsyn kan brukes av virksomheter for å løfte kunnskapen om potensielle cybertrusler og bedre sin beredskap mot dem. Artikkelen bygger på analyse av litteratur om risikostyring, cybertrusler og framsyn med hovedvekt på scenarioanalyse. Drøftelsen illustrerer at scenarioanalyse kan være et nyttig verktøy for å sette virksomheten i stand til å lære mer om de ukjente cybertruslene. Dette kan stimulere til kontinuerlig organisatorisk læring for å bedre beredskapen mot potensielle cybertrusler.

Artikkelen tar først for seg kritikk av tradisjonell risikostyring. Deretter beskrives essensen i framsyn gjennom scenarioanalyse. Videre følger en diskusjon om hvordan scenarioanalyser kan møte kritikken av tradisjonell risikostyring. Avslutningsvis presenteres tre dilemmaer og fallgruver med scenarioanalyser, før konklusjon og behov for framtidig forskning.

KRITIKKEN AV TRADISJONELL RISIKOSTYRING

Risikostyring er i utgangspunktet ment for å hjelpe ledere med å håndtere usikkerhet. Det finnes mange normative rammeverk, fra for eksempel COSO og ISO, som framstiller tradisjonell risikostyring som en rasjonell prosess. I disse rammeverkene kan risikoen objektivt dokumenteres, måles, analyseres, rapporteres og revideres. Informasjon kan danne grunnlag for en virksomhets risikostyring. Tradisjonell risikostyring har til hensikt å avdekke uønskede hendelser og på den måten hindre at hendelsene inntreffer og truer virksomhetens måloppnåelse. Uønskede hendelser kan være alt fra datamanipulasjon og sabotasje til misligheter og svindel. Den tradisjonelle løsningen på problemene eller de uønskede hendelsene er å innføre rutinebasert risikostyring med sjekklister for å påse at regler og rutiner er på plass og fungerer (Moeller, 2011, s. 132). I de tilfellene hvor en uønsket hendelse likevel har inntruffet, kan man lære av egne feil og sette i verk bedre rutiner. Det er også slik at veldokumentert risikostyring er en legitimeringssak, fordi mange eksterne aktører, særlig myndighetene, ofte stiller krav til internkontroll og risikostyringssystemer. Av erfaring er det ofte slik at virksomheter kun tilfredsstiller minstekrav til slike systemer, og ikke gjør tiltak eller arbeid utover det de er pålagt. Utover dette har praktisering av tradisjonell risikostyring fått mye kritikk i risikostyringslitteraturen. Vi trekker her fram to: At tradisjonell risikostyring kan skape en illusjon om kontroll, og at den ikke er effektiv mot alle typer risiko, spesielt såkalte sorte svaner.

TRADISJONELL RISIKOSTYRING SKAPER EN ILLUSJON OM KONTROLL

Power (2009) argumenterer for at ambisjonen med risikostyring – å risikostyre alt – i virkeligheten kan gi motsatt effekt – risikostyring av ingenting. Mange ledere kan operere i tilstander vi betegner som en illusjon om kontroll. I dette ligger at mange har en tilbøyelighet til å overvurdere egen påvirkningsevne og kontroll. Her er troen på at man kan kontrollere risiko og påvirke framtidige positive resultater for sin virksomhet, større enn hva det objektivt sett er grunnlag for å anta (Schwenk, 1984, s. 121–122). Næringslivets sikkerhetsråd (2019, s. 12–13) fant en lignende tendens i sin undersøkelse av hybride trusler. Undersøkelsen

avdekket at 61 prosent av virksomhetene vurderer det som vanlig å bli utsatt for hybride angrep, til tross for at langt færre, 24 prosent, anså det som sannsynlig at deres egen virksomhet blir rammet. Illusjonen om kontroll over cybertrusler kan forsterkes av programvare, avtaler med anerkjente IT-miljøer og interne rutiner. Eksempelvis kan høy tiltro til leverandøren føre til at relevante spørsmål ikke blir stilt (Ceric & Holland, 2019, s. 183). Som resultat er evnen til objektiv vurdering av potensielle trusler og framtidige angrep sterkt redusert, og operative beslutninger tas på mangelfullt grunnlag.

I møte med cybertrusler kan menneskelige kognitive skjevheter medføre at tradisjonell risikostyring kommer til kort. Ulike kognitive skjevheter kan også virke sammen og ha en forsterkende effekt på hverandre. Bevisstgjøring rundt dette kan med andre ord påvirke risikostyringen. En utfordring er likevel at mennesker har begrenset kapasitet til å prosessere informasjon (Ceric & Holland, 2019, s. 183–184). Ikke-spesialister har i tillegg ofte problemer med å forstå de tekniske sidene ved cybertrusler, og det kan derfor bli krevende å ta gode beslutninger. Kognitiv skjevhetet medfører at beslutningstakere istedenfor å søke ny kunnskap, ekspertise og informasjon, heller strukturerer en problembeskrivelse og løsning basert på informasjon som støtter deres egne erfaringer, konklusjoner og fortolkninger (Ceric & Holland, 2019, s. 174).

Ifølge Soin og Collier (2013) bærer risikostyringen i enkelte virksomheter preg av sjekklister som ikke påvirker daglig drift, men skal demonstrere at interne rutiner er i samsvar med eksterne retningslinjer og krav. I slike tilfeller er risikostyringen først og fremst et legitimeringsverktøy – en illusjon om kontroll og en måte å oppnå legitimitet og gi ryggdekning på ved eventuelle hendelser. Det kan være sterke insentiver for å opprettholde en illusjon om kontroll både innad og utad. Graden av kontroll som investorer, myndigheter, kunder, konkurrenter og ansatte opplever, kan være avgjørende for forretningsmessige formål. I andre tilfeller kan manglende overvåkning og rapportering gi en illusjon av kontroll fordi eventuelle hendelser og trusler ikke kommer fram.

Paradoksalt nok kan det være vanskelig å sikre investeringer i cybersikkerhet fordi målet med tiltakene er at man *ikke* skal merke noe, eller at tiltakene *ikke* medfører noen merkbar konsekvens, det vil si fravær av hendelser. Det er heller motsatt: at avdelinger som utsettes for angrep, kan peke på manglende ressurser og oppnå økte budsjetter for å arbeide med sikkerhetstiltak etter at uhellet har vært ute.

TRADISJONELL RISIKOSTYRING ER LITE EFFEKTIV, SÆRLIG MOT SORTE SVANER

Risiko finnes i ulike former. Tradisjonell risikoanalyse, som beslutningstrær, forventet nytte og bayesiansk statistikk, er best egnet til å håndtere risiko i stabile omgivelser (Schoemaker, 1993, s. 208). De er med andre ord lite egnet til å håndtere høy usikkerhet og sorte svaner – de helt uventede hendelsene.Innen tradisjonell risikostyring forutsettes det ofte at uønskede hendelser kan dokumenteres, kvantifiseres og måles før det gjøres statistiske analyser av sannsynligheter og konsekvenser. På den måten vektlegger tradisjonell risikostyring hendelser som lar seg kvantifisere, dokumentere og kontrollere (Power, 2009, s. 851–852). I en verden som er blitt mer og mer kompleks som følge av blant annet ny teknologi, kan man godt lure på om omfanget av risikoer som faller under sorte svaner, øker betraktelig. Særlig gjelder dette cybertrusler. Manglende kunnskap om hendelser er et problem blant virksomhetene, også innen kritisk infrastruktur. I mange tilfeller kjenner ikke ofrene årsaken til at hendelsen inntraff (Norges vassdrags- og energidirektorat, 2017, s. 19–20). Det er også betydelig usikkerhet forbundet med når, hvor, hvordan og hvorfor de neste cyberhendelsene vil inntreffe, og hvem kan stå bak disse.

Det er viktig å merke seg at håndtering av kjente risikoer til en viss grad kan automatiseres. Dette gjelder også programvare som for eksempel kan blokkere e-post som lett lar seg identifisere som søppelpost eller svindelforsøk. Derimot må vellykkede angrep og arbeid med sorte svaner ses i sammenheng med det menneskelige aspektet. Tall fra Proofpoint (2019, s. 2) viser at under én prosent av angrepene via e-post som de observerte, benyttet systemsårbarheter. De resterende 99 prosentene utnyttet menneskelige faktorer som nysgjerrighet og tillit. Det er nettopp den menneskelige faktoren som gjør situasjonen uforutsigbar (Ceric & Holland, 2019, s. 184). Dette taler for en bredere forståelse av cybertrusler hvor enhver virksomhet kan betraktes som en del av et sosialt system med ulike menneskelige aktører. Når mennesker spiller en avgjørende rolle i vellykkede angrep, må også

mennesker være sentrale i å utforme systemer for å møte sorte svaner.

Oppsummert er det et behov for å bevege risikostyring fra etterlevelse av regler og sjekklister til gjennomtenkte ideer om potensielle framtidsscenarioer (Power, 2009, s. 852). Vi mener tradisjonell, reaktiv risikostyring er utilstrekkelig, især i situasjoner hvor kognitive skjevheter forsterker en illusjon om kontroll, og i møte med sorte svaner. Cybertrusler er ikke bare tekniske, men har også en menneskelig dimensjon. Håndtering av cybertrusler er dermed en sosial prosess hvor ensidig oppmerksomhet om teknologi kan hindre virksomheter i å oppfatte og forstå kritiske trusler (Parenty & Domet, 2019). I neste del skal vi se på hvordan framsyn og spesielt scenarioanalyse kan framstå som et viktig supplement, om ikke alternativ, til tradisjonell risikostyring.

FRAMSYN GJENNOM SCENARIOANALYSER: HVA OG HVORFOR?

Scenarioer kan ha ulike betydninger. For ingeniører eller sikkerhetseksperter indikerer begrepet i hvilken operasjonell kontekst ulike typer simuleringer, for eksempel beredskapsøvelser, finner sted (Schoemaker, 1993, s. 194–195). Når vi introduserer begrepet scenarioer i denne artikkelen, mener vi noe annet. Scenarioer er sammenhengende og troverdige beskrivelser om framtiden, og ikke operasjonelle kontekster, «projeksjoner, prediksjoner eller preferanser» (Cornelius, Van de Putte, & Romani, 2005, s. 93). Scenarioer er historier eller bilder av potensielle framtider som skapes gjennom anvendelse av framsyn som metode.

Scenarioanalyse er én av flere metoder for å arbeide med framsyn. I denne artikkelen brukes den intuitive logiske metoden, ofte kalt Shell-metoden, som beskrevet av Amer, Daim og Jetter (2013, s. 26–28). Arbeidet struktureres ved at diskusjonsgrupper identifiserer en rekke viktige faktorer, som økonomi, trender, politikk med flere, som kan forme framtidig utvikling. Metoden er således prisgitt gruppemedlemmenes kunnskap, evner og engasjement. Resultatet skal være troverdige beskrivelser av potensielle framtider. Slik blir beslutningstakere mer oppmerksomme på potensielle endringer i omgivelsene og hvordan disse kan møtes. Metoden er primært kvalitativ og egnet til å beskrive scenarioer som ikke lar seg modellere kvantitativt (Pollard & Hotho, 2006, s. 728). Det henvises til Amer og medforfattere (2013) for de som ønsker å fordype seg i ulike metoder.

UTFORDRE MENTALE MODELLER

Utover at scenarioer i seg selv er ment å være resultatet av framsyn, har scenarioer også andre formål. Som mennesker har vi en tendens til å tenke at framtiden kommer til å ligne nåtiden. Det er derimot ingen garanti for at framtiden, særlig i bransjer preget av høyt endringstempo, kommer til å ligne nåtiden. Scenarioer er et verktøy for å endre mentale modeller slik at virksomheten både kognitivt og kollektivt er bedre forberedt på å håndtere usikkerhet i omgivelsene. For å oppnå dette må scenarioene være sterke, troverdige og gjerne rikt beskrevet med detaljer (Schoemaker, 1993, s. 201–202). Dette åpner muligheten for å diskutere og korrigere antagelser og utarbeide forslag til reviderte strategier og innsatsplaner. Det er omdiskutert om scenarioanalyse faktisk klarer dette, og empiriske funn tilsier at scenarioanalyse har motsatt effekt, altså forsterkende effekt, på eksisterende antagelser og mentale modeller (Balarezo & Nielsen, 2017, s. 15–16).

TIDLIG VARSLING

Scenarioer er også ment å fungere som et system for tidlig varsling ved å stimulere til å identifisere potensielle trusler samt hvordan virksomheten kan respondere på ulike framtidige trusler og muligheter (Cornelius mfl., 2005, s. 95; Marshall mfl., 2019, s. 650). Dette betyr ikke at tidlig varsling gir noen garanti for effektiv risikostyring. Scenarioer skal ikke gi en følelse av kontroll over framtiden, men heller en bedre forståelse av mulige farer og en bevisstgjøring om at vår forståelse av samfunnet og handlinger er mangelfull (McDermott, 1996, s. 191, 194). Dette gjør at scenarioanalyse kan ha en viktig funksjon i å identifisere hendelser og utarbeide beredskapsplaner.

LÆRING

Scenarioer er ment for å skape læring. Økt bevissthet, forståelse og læring, som igjen skal gi bedre beslutninger og drift, skal være noen av resultatene av scenarioanalyse. På den måten framstår scenarioanalyse som et verktøy for å skape kontinuerlig læring i virksomheten. Dette gjelder på både virksomhetsnivå og individnivå (Balarezo & Nielsen, 2017, s. 9). Gjennom identifisering

og beskrivelse av (sjeldne) framtidige hendelser skal kognitiv treghet ved endringer reduseres.

Oppsummert er scenarioanalyse en prosess for organisatorisk intervensjon og læring om potensielle framtider som kan redusere svakhetene i tradisjonell risikostyring. I neste del ser vi på hvordan scenarioanalyse kan bistå med å bedre cybersikkerhet.

SCENARIOANALYSE SOM RISIKORADAR MOT CYBERTRUSLER

Det er mange grunner til at cybersikkerhet skal stå høyt på agendaen hos virksomhetsledere. I følge flere nasjonale og internasjonale retningslinjer skal cybersikkerhet inngå som en del av virksomhetsstyrenes overordnede ansvar for risikostyring og internkontroll. Dermed må man vurdere hvordan cybertrusler kan påvirke forretningsmessige aktiviteter i virksomheten. Siden cyberhendelser kan gi betydelige negative effekter for hele virksomheten, blir vurdering av cyberrisiko for viktig til at den kan overlates kun til IT-eksperter og eventuelt personell som arbeider direkte med cybersikkerhet. Parenty og Domet (2019) anbefaler at hver virksomhet skal utarbeide det de kaller cybertrusselhistorier. Historiene skal hjelpe virksomhetene med å oppdage trusler og prioritere og forberede mottiltak. Gruppa som skal utvikle historiene, skal bestå av ledere på ulike nivå, personell på operasjonsnivå, ansvarlige for IT-systemer samt andre relevante spesialister på de ulike områdene. Metoden adresserer systematisk koblinger mellom 1) kritiske forretningsmessige aktiviteter, 2) eksisterende IT-systemer, 3) cyberangrep og konsekvenser disse kan ha for virksomheten, og 4) gjerningspersoner, deres motivasjon og evner.

Metaforisk kan scenarioanalyse presenteres som en risikoradar. Radarmetaforen er hentet fra militær etterretning. Radaren kan ses på som et verktøy for proaktiv skanning av omgivelser for å oppdage og overvåke selv svake signaler om cybertrusler for å håndtere dem bedre. Radaren kan lokaliseres og posisjoneres i den nødvendige retningen. Med dette menes at scenariodiskusjoner kan rettes mot spesifikke temaer og analyseenheter. Ideen er at radaren kan forsterkes til å undersøke for eksempel en virksomhets sosiale trusselbilde. (Marshall mfl., 2019, s. 645, 650)

Siden cybertrusler har betydning for både strategisk og operasjonelt nivå, krever scenarioanalyse samhandling mellom ulike nivå i en virksomhet eller gruppe (Parenty & Domet, 2019). Overordnet nivå skal identifisere trusler som representerer en strategisk utfordring. Operasjonelt nivå skal identifisere trusler av operasjonell karakter og hvordan disse kan møtes. Dette krever samarbeid og kreativ tenkning i virksomheten og effektiv kunnskapsdeling mellom nivåene. En slik kunnskapsdeling kan foregå ved å etablere grupper som møtes regelmessig. Siden scenarioanalyse krever innspill fra individer, og noe arbeid dermed er individualisert, krever dette konstant utvikling av kompetanse hos ansatte, noe som i sin tur vil bidra til å forbedre kvaliteten på informasjon om usikkerheter og muliggjøre kreativ fortolkning av tilgjengelig informasjon.

Resultater av samhandlingsgrupper for scenarioanalyse kan være overordnede scenarioer som suppleres med en liste med operative innsatsplaner for ulike typer cyberangrep. Videre kan virksomheter teste slike innsatsplaner gjennom rollespill hvor hvert av scenarioene testes gjennom simuleringer og beredskapsøvelser. Dette kan bidra til bedre læring for eksempel gjennom koding av resultatene av rollespillet inn i reviderte innsatsplaner. (Marshall mfl., 2019, s. 655)

Det er kjent at scenarioanalyse blir brukt i norske virksomheter i ulike bransjer (Bourmistrov, Helle, & Kaarbøe, 2017). Vi har likevel begrenset kunnskap om hvordan scenarioer brukes, og kan brukes, til å bedre cybersikkerhet både i teori og praksis. Vi argumenterer for at framsyn og scenarioanalyse kan hjelpe virksomheter til å se styring av cybertrusler som en sosial prosess, og på den måten unngå en illusjon om kontroll.

FRAMSYN FOR CYBERSIKKERHET: POTENSIELLE DILEMMAER OG FALLGRUVER

Etter vår vurdering har bruken av framsyn og scenarioanalyse i virksomheter generelt positiv omtale i litteraturen. Det er likevel flere temaer hvor mer forskning er nødvendig for å klargjøre effekter av scenarioanalyse (Balarezo & Nielsen, 2017, s. 15–19; Amsteus, 2008, s. 63). Med tanke på dette ønsker vi å trekke fram tre potensielle dilemmaer og fallgruver for virksomheter. Vi anbefaler at også praktikere er oppmerksomme på disse, da de kan skape problemer for praksis. Dette gjelder organisatorisk grensearbeid, selvoppfyllende profetier og paranoide organisasjoner.

ORGANISATORISK GRENSEARBEID

Bruken av scenarioanalyse krever en diskusjon rundt hvem som skal være involvert i gruppa som skal produsere scenarioene. Som nevnt er gruppesammensetningen avgjørende for arbeidets resultat. En gruppe bestående av kun internt ansatte er det vanligste i den intuitive logiske metoden (Amer mfl., 2013, s. 28). Alternativt kan det åpnes for eksterne, for eksempel gjennom samarbeid med flere aktører i samme bransje. En tredje mulighet er å involvere flere interne eller eksterne interessenter, som myndigheter, kunder og leverandører. En fjerde mulighet er nettdugnad – hvor prosessen er åpen for alle. Det finnes ingen fasit her. Mens bred involvering av flere parter kan være gunstig for å få fram de viktigste perspektivene (Parenty & Domet, 2019; Schoemaker, 1993, s. 200), er dette også kostnads- og ressurskrevende for en virksomhet. Gieryn illustrerer at grensa for hva som skal tas inn i en profesjonell praksis eller ikke, er i endring. Med eksempler fra vitenskapen og akademia viser han at det også kan være insentiver for å holde seg til en engere krets, for eksempel for å unngå ansvar, bevare egen autonomi eller oppnå monopol på ressurser og profesjonell autoritet (Gieryn, 1983, s. 791–792). Litteraturen diskuterer også under hvilke omstendigheter samarbeid mellom virksomheter kan være hensiktsmessig (Wiener, Gattringer, & Strehl, 2018). Dette er særlig relevant for vurdering av cybertrusler. Det kan være behov for utvidet grensearbeid ved for eksempel å engasjere tidligere kriminelle og/eller opprette kommunikasjon med avanserte hackermiljøer (Marshall mfl., 2019, s. 645). Dette skaper uten tvil store etiske dilemmaer som må diskuteres og adresseres.

SELVOPPFYLLENDE PROFETIER

En selvoppfyllende profeti oppstår når forventningen til en hendelse skaper en atferd som øker sannsynligheten for at hendelsen inntreffer. Om vi ser på scenarioer som en teori om framtidige hendelsesforløp, kan det ifølge Ferraro, Pfeffer og Sutton (2005) være fare for at et bestemt scenario vinner tilhørere og etter hvert påvirker hvordan institusjonelt design og lederpraksis formes. Dette er fordi en institusjonalisert teori kan ha stor påvirkning på ideer, forutsetninger og bruken av profesjonelt språk. Det er absolutt en mulighet at virksomheter, særlig om de benytter seg av scenarioanalyse, avdekker en potensiell framtid som blir viet stor oppmerksomhet, og som gradvis muliggjør kollektiv handling, ikke bare internt, men også blant aktører utenfor virksomheten. Gjennom kollektive handlinger kan aktørene sammen påvirke til at nettopp en bestemt framtid materialiserer seg. Dette kan skje ved at et skadescenario lekker ut av virksomheten og gir hackermiljøer ideer til nye angrep.

PARANOIDE ORGANISASJONER

Overdreven konsentrasjon om ugunstige potensielle scenarioer kan gi tilsvarende sterk bekymring for at scenarioet skal inntreffe. Trusselbilder kan således generere vrangforestillinger om faktisk risiko, spesielt i tilfeller hvor relevant informasjon blir neglisjert (Schwarz, 2007, s. 20). Dette betegner vi som paranoide organisasjoner. Virksomheter kan spore av mot kontinuerlige søk etter andres skjulte hensikter og på den måten fremme mistillit og mistenksomhet. Når scenarioene skal diskuteres, kan slike virksomheter være så besatt av spesifikke framtider at de overproduserer negative bilder av nåtiden og framtiden, og overser alternative og for eksempel mer positive framtider, slik at disse ikke tas med videre i virksomhetens planer.

KONKLUSJON

Formålet med denne artikkelen var å diskutere hvordan framsyn kan brukes av virksomheter til å løfte kunnskapen om potensielle cybertrusler og øke sin beredskap. Gjennom analysen av litteraturen om både risikostyring og framsyn konkluderer vi med at bruken av scenarioanalyse som framsyn bør vurderes av virksomheter. Metoden trenger ikke erstatte tradisjonelle verktøy for risikostyring, men kan være et viktig supplement. Scenarioanalyse kan fungere som en risikoradar for å gi tidlig varsling om eventuelle hendelser og bidra til å redusere illusjonen om kontroll, siden potensielle trusler kan diskuteres i virksomheten på en systematisk måte av beslutningstakere og redusere kognitive skjevheter. Dette skjer gjennom å utfordre ledere og ansatte til å tenke proaktivt om cybertrusler og beredskap på både overordnet nivå, som hvordan cybersikkerhet passer inn i forretningsstrategien, og på operasjonelt nivå, som hvilken kombinasjon av innsatsplaner og tiltak som kan iverksettes gitt ulike scenarioer. Dette kan løfte kunnskapen om, og bedre beredskapen mot, potensielle cybertrusler. Vi advarer også om potensielle dilemmaer og fallgruver som er viktige å reflektere over ved scenarioanalyse, herunder

rollen risikostyring har i organisatorisk grensearbeid, selvoppfyllende profetier og paranoide organisasjoner.

Selv om det er gjennomført betydelig forskning på risikostyring, framsyn og cybersikkerhet hver for seg, har vi begrenset kunnskap om hvordan scenarioer som en del av risikostyring kan gi bedre cybersikkerhet. Vi etterlyser mer forskning som beskriver og analyserer beste praksis, for eksempel i virksomheter som allerede har tatt i bruk scenarioanalyse med positive eller negative resultater. Det kunne også vært interessant å benytte aksjonsforskning som metode på dette området, for eksempel ved at forskere i samarbeid med virksomhetene implementerer scenarioanalyse med formål om å bedre cybersikkerheten. M

REFERANSER

Amer, M., Daim, T.U., & Jetter, A. (2013). A review of scenario planning. *Futures*, *46*, 23–40. https://doi.org/10.1016/j.futures.2012.10.003

Amsteus, M. (2008). Managerial foresight: Concept and measurement. *Foresight*, *10*(1), 53–66. https://doi.org/10.1108/14636680810856026

Balarezo, J., & Nielsen, B.B. (2017). Scenario planning as organizational intervention: An integrative framework and future research directions. *Review of International Business and Strategy*, *27*(1), 2–52. https://doi.org/10.1108/RIBS-09-2016-0049

Bourmistrov, A., Helle, G., & Kaarbøe, K. (2017). Kreativ tenkning eller intelligent maskin? *Praktisk økonomi & finans*, *33*(1), 69–85. https://doi.org/10.18261/issn.1504-2871-2017-01-06

Ceric, A., & Holland, P. (2019). The role of cognitive biases in anticipating and responding to cyberattacks. *Information Technology and People*, *32*(1), 171–188. https://doi.org/10.1108/ITP-11-2017-0390

Cornelius, P., Van de Putte, A., & Romani, M. (2005). Three decades of scenario planning in Shell. *California Management Review*, *48*(1), 92–109.

Ferraro, F., Pfeffer, J., & Sutton, R.I. (2005). Economics language and assumptions: How theories can become self-fulfilling. *Academy of Management Review*, *30*(1), 8–24. Hentet 27.02.2020 fra http://jeffreypfeffer.com/wp-content/uploads/2011/10/AMR-Jan2005.pdf

Gieryn, T.F. (1983). Boundary-work and the demarcation of science from non-science: Strains and interests in professional ideologies of scientists. *American Sociological Review*, *48*(6), 781–795. Hentet 27.02.2020 fra https://www.jstor.org/stable/2095325

Kulset, E.M., & Meidelsen, K.H.R. (2020). Internkontroll som virkemiddel for å hindre underslag og svindel på innkjøpsområdet. *Magma*, *23*(1), 47–56.

Leitch, M. (2008). *Intelligent internal control and risk management: Designing high-performance risk control systems*. Aldershot: Gower.

Marshall, A., Ojiako, U., Wang, V., Lin, F., & Chipulu, M. (2019). Forecasting unknown-unknowns by boosting the risk radar within the risk intelligent organisation. *International Journal of Forecasting*, *35*(2), 644–658. https://doi.org/10.1016/j.ijforecast.2018.07.015

McDermott, W.B. (1996). Foresight is an illusion. *Long Range Planning*, *29*(2), 190–194. https://doi.org/10.1016/0024-6301(96)00007-6

Moeller, R.R. (2011). *COSO enterprise risk management: Establishing effective governance, risk, and compliance processes* (2. utgave). Hoboken: Wiley.

Næringslivets sikkerhetsråd. (2019). *Hybridundersøkelsen: Hybride trusler og hendelser mot norsk næringsliv*. Hentet 19.08.2019 fra https://www.nsr-org.no/getfile.php/1312167-1553166117/Dokumenter/NSR publikasjoner/Hybridundersøkelsen/Hybridundersøkelsen_web.pdf

Norges vassdrags- og energidirektorat. (2017). *Informasjonssikkerhetstilstanden i energiforsyningen*. Oslo. Hentet 21.06.2018 fra http://publikasjoner.nve.no/rapport/2017/rapport2017_90.pdf

Parenty, T.J., & Domet, J.J. (2019). Sizing up your cyberrisks. *Harvard Business Review*, *97*(6), 102–109. Hentet 27.02.2020 fra http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=139017616&lang=es&site=ehost-live

Pollard, D., & Hotho, S. (2006). Crises, scenarios and the strategic management process. *Management Decision*, *44*(6), 721–736. https://doi.org/10.1108/00251740610673297

Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society*, *34*(6–7), 849–855. https://doi.org/10.1016/j.aos.2009.06.001

Proofpoint. (2019). *Human factor report 2019*. Hentet 12.09.2019 fra https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf

Schoemaker, P. (1993). Multiple scenario development: Its conceptual and behavioral foundation. *Strategic management journal*, *14*(3), 193–213. https://doi.org/10.1002/smj.4250140304

Schwarz, J.O. (2007). Assessing future disorders in organizations: Implications for diagnosing and treating schizophrenic, depressive or paranoid organizations. *Foresight*, *9*, 15–26.

Schwenk, C.R. (1984). Cognitive simplification processes in strategic decision-making. *Strategic Management Journal*, *5*(2), 111–128.

Soin, K., & Collier, P. (2013). Risk and risk management in management accounting and control. *Management Accounting Research*, *24*(2), 82–87. https://doi.org/10.1016/j.mar.2013.04.003

Wiener, M., Gattringer, R., & Strehl, F. (2018). Participation in inter-organisational collaborative open foresight. A matter of culture. *Technology Analysis & Strategic Management*, *30*(6), 684–700. https://doi.org/10.1080/09537325.2017.1376045

Utgitt i ph.d. serie ved Handelshøgskolen:

Nr. 1 – 2003 Lars Øystein Widding
Bygging av kunnskapsreservoarer i teknologibaserte nyetableringer

Nr. 2 – 2005 Pawan Adhikari
Government Accounting in Nepal: Tracing the Past and the Present

Nr. 3 – 2005 Tor Korneliussen
The Relationship between Initation, Barriers, Product Quality and Internationalization

Nr. 4 – 2005 Bjørn Willy Åmo
Employee innovation behavior

Nr. 5 – 2005 Odd Birger Hansen
Regnskap og entreprenørskap. En fortolkende studie av hvordan to entreprenører bruker regnskap

Nr. 6 – 2006 Espen John Isaksen
Early Business Performance
- Initial factors effecting new business outcomes

Nr. 7 – 2006 Konstantin Timoshenko
Russian Government Accounting:
Changes at the Central level and at a University

Nr. 8 – 2006 Einar Rasmussen
Facilitating university spin-off ventures
-an entrepreneurship process perspective

Nr. 9 – 2007 Gry Agnete Alsos
Portfolio Entrepreneurship - general and farm contexts

Nr. 10 – 2007 Elsa Solstad
Tre sykehus - to verdener - en fusjon.
En studie av reorganisering i et helseforetak

Nr. 11 – 2007 Levi Gårseth-Nesbakk
Experimentation with accrual accounting at the central government level in Norway - how a global phenomenon becomes a local practice

Nr. 12 – 2007 Tatiana Iakovleva
Factors Associated with new venture performance:
The context of St. Petersburg

Nr. 13 – 2007 Einar Lier Madsen
Utvikling av dynamiske kapabiliteter i små og mellomstore bedrifter

Nr. 14 – 2008 Anne Haugen Gausdal
'Network Reflection' – a road to regional learning, trust and innovation

Nr. 15 – 2008 Lars Rønning
Social capital in farm-based entrepreneurship and rural development

Nr. 16 – 2008 Terje Andreas Mathisen
Public Passenger Transport in Norway – Regulation, Operators' Cost Structure and Passengers' Travel Costs

Nr. 17 – 2008 Evgueni Vinogradov
Immigrant Entrepreneurship in Norway

Nr. 18 – 2008 Elin Oftedal
Legitimacy of Creative Destruction

Nr. 19 – 2009 Frode Kjærland
Valuation of Generation Assets – a Real Option Approach

Nr. 20 – 2009 Tatiana Maximova-Mentzoni
Marketization of the Russian University: Origins, Features and Outcomes

Nr. 21– 2009 Hugo Skålsvik
Studies of Market led Processes influencing Service Performance:
-Case Studies on the Norwegian Coastal Voyage

Nr. 22– 2009 Svein Oskar Lauvsnes
Determinants of a shifting effective demand equilibrium.
An explorative investigation of the interaction between
psychological, financial and real factors

Nr. 23– 2010 Frode Fjelldal-Soelberg
Entreprenøriell markedsføring. En studie av entreprenørskap og markedsføring som overlappende fenomen

Nr. 24– 2010 Heidi Rapp Nilsen
From Weak to Strong Sustainable Development
An analysis of Norwegian economic policy tools in mitigating climate change

Nr. 25– 2010 Gowindage Chamara Jayanath Kuruppu
Development of Central Government Accounting in Sri Lanka:
Three perspectives on the accounting changes

Nr. 26– 2010 Marina Z. Solesvik
Interfirm collaboration: The context of shipbuilding.

Nr. 27– 2010 Jan Terje Henriksen
Planning, Action and Outcome
- Evaluation of the Norwegian Petroleum System:
A Structuration Approach to Ripple Effect Studies

Nr. 28– 2010 May Kristin Vespestad
Empowered by Natures – Nature-based High North Tourism Experiences in an International Context

Nr. 29– 2011 Andrei Mineev
How has the petroleum supply industry developed in The Russian Barents Sea Region? Institutional and managerial aspects

Nr. 30– 2011 Jorunn Grande
Entrepreneurship in small rural firms - the case of agriculture

Nr. 31– 2011 Thomas Johansen
Paradigms in Environmental Management Research:
Outline of an Ecosophical-Hermeneutic Alternative

Nr. 32– 2011 Elena Dybtsyna
Accountant in Russia: changing times, changing roles.

Nr. 33– 2012 Harald Fardal
Information Systems Strategy in Practice
A Social Process Perspective

Nr. 34– 2012 Kristin Haugland Smith
Hva er bedrifters samfunnsansvar?
- En empirisk tilnærming av bedrifters ansvar overfor samfunnet

Nr. 35– 2012 Are Branstad
The management of entrepreneurship support
– Organisation and learning in corporate incubation, technology transfer and venture capital

Nr. 36– 2012 Victoria Konovalenko
A “coordination kaleidoscope”:
The role of a “Corporate University” as a coordinator of knowledge flows in a Russian transnational corporation

Nr. 37– 2012 Thor-Erik Sandberg Hanssen
Essays in Transport Economics with application to Transport Policy

Nr. 38– 2013 Are Severin Ingulfsvann
Verdiforskyvning i friluftslivet i lys av økologisk økonomi

Nr. 39– 2013 Natalia Andreassen
Sustainability Reporting in a Large Russian Oil Corporation.
Production Safety Issues

Nr. 40– 2013 Elena Panteleeva
Contemporary Management Accounting Practices in Russia:
The Case of a Subsidiary in a Russian Oil Company

Nr. 41– 2013 Thusitha S.L.W.Gunawardana
Impact of Power Sources on Channel Members' Performance

Nr. 42– 2013 Nadezda Nazarova
Mastering Nature and Managing Frictions: Institutional Work and Supply Chain Management in the High North

Nr. 43– 2013 Inge Hermanrud
Managed Networks of Competence in Distributed Organizations
- The role of ICT and Identity Construction in Knowledge Sharing

Nr. 44– 2013 Kari Djupdal
Sustainable entrepreneurship:
outcomes associated with an environmental certification resource

Nr. 45– 2013 Imtiaz Badshah
Federal government accounting in The Islamic Republic of Pakistan

Nr. 46– 2014 Muhammad Arif
Inter-organizational Exchange Relationships
– Exchange Relationships between Local Service Suppliers and Tour Operators in the Tourism Distribution Channel

Nr. 47– 2014 Wondwesen Tafesse
The Marketing Functions of the Trade Show System

Nr. 48– 2014 Fritz J. Nilssen
Erfaringsutveksling som grunnlag for mestring og livskvalitet
Diagnoseoverskridende samtalegrupper for familier med barn som har nedsatt funksjonsevne og eller kronisk sykdom.

Nr. 49– 2014 Ingebjørg Vestrum
The Resource Mobilisation Process of Community Ventures
-The Case of Cultural Events in Rural Communities

Nr. 50– 2014 Ragnhild Johnson
The Practice of Project Management
- A qualitative analysis of complex project-based organizations

Nr. 51– 2014 Ann Heidi Hansen
Memorable moments
Consumer immersion in nature-based tourist experiences

Nr. 52– 2014 June Borge Doornich
Entry modes and organizational learning during internationalization
An analysis of Norwegian supply companies' entering and expanding in the Russian oil and gas sector

Nr. 53– 2014 Kjersti Karijord Smørvik
Opplevelsesskaping i dynamiske opplevelsesrom:
En studie av turisters opplevelser på Hurtigruten

Nr. 54– 2015 Marianne Terese Steinmo
How Firms use University-Industry Collaboration to Innovate:
The role and Development of Social Capital and Proximity Dimensions

Nr. 55– 2015 Eva J.B. Jørgensen
Border Firms: Norway and Russia

Nr. 56– 2015 Krister Salamonsen
Exogenous Shocks as Drivers of Growth in Peripheral Regions.
- A Multilevel Approach to Regional Development

Nr. 57– 2015 Hindertje Hoarau Heemstra
Practicing open innovation in experience-based tourism:
the roles of knowledge, values and reflexivity

Nr. 58– 2015 Elena Zhurova
Environmental Performance Reporting of Russian Oil and Gas Companies

Nr. 59– 2016 Siri Jakobsen
Environmental innovation cooperation:
The development of cooperative relationships between Norwegian firms

Nr. 60– 2016 Antonina Tsvetkova
Supply Chain Management in the Russian Arctic:
An institutional perspective

Nr. 61– 2017 Kjersti Granås Bardal
Impact of Adverse Weather on Road Transport:
Implications for Cost-Benefit Analysis

Nr. 62– 2017 Kristian Støre
Methodological contributions and applications in real options analysis

Nr. 63– 2017 Thomas André Lauvås
The dynamics of university-industry collaboration:
A longitudinal case study of research centers

Nr. 64– 2017 Sølvi Solvoll
Development of effectual and casual behaviors:
Exploring new venture creation in the tourism industry

Nr. 65– 2017 Evgenii Aleksandrov
The changing role of accounting from reformees' perspective:
A study of public sector reforms in Russia

Nr. 66– 2017 Igor Khodachek
Budget, Strategy and Accounting.
Managing institutional change in Russia's governments

Nr. 67– 2018 Vivi Marie Lademoe Storsletten
Quality as flourishing
A study of quality based upon leadership in kindergartens with implications for Ecological Economics

Nr. 68– 2018 Olga Iermolenko
The human side of accounting:
The bonds between human agency and management accounting practices' changes in the transitional economy

Nr. 69– 2018 Karin Wigger
Mobilization of Collective Resources for Entrepreneurship:
Case Studies in Nordic Peripheries

Nr. 70 – 2018 Andreas Mikkelsen
Trading fast and slow: algorithmic trading in the Nordic region

Nr. 71 – 2018 Asbjørn Veidal
Strategic entrepreneurship in farm businesses

Nr. 72 – 2018 Are Jensen
Early imprints in and on new technology-based firms

Nr. 73 – 2018 Marianne Arntzen-Nordqvist
The financing process of new technology-based firms
- The entrepreneur's perspective

Nr. 74 – 2019 Irina Nikolskaja Roddvik
Deprivation of control: A driving force to gain influence during the internationalization process of MNC

Nr. 75 – 2019 Petter Gullmark
Unraveling the Building Blocks of Local Government Organizations' Innovativeness: Insights from a Dynamic Capabilities Perspective

Nr. 76 – 2019 Hanne Stokvik
Knowledge for Innovation

Nr. 77 – 2019 Anastasiya Henk
Between the Devil and the Deep Blue Sea: Managing Business Processes in Turbulent Environments

Nr. 78 – 2019 Tadeu Fernando Nogueira
Entrepreneurial Learning: An Exploration of the Learning of New Venture Founders

Nr. 79 – 2020 Veronika Vakulenko
Public Sector Reforms in Ukraine: Roles Played by Global and Local Agents in Implementing Converging and Diverging Changes

Nr. 80 – 2020 Lars Hovdan Molden
Adapting to Change - On the Mechanisms of Dynamic Capabilities

Nr. 81 – 2020 Sudip Kranti Tiwari
Navigating International Entrepreneurship in a Developing Economy Context: Lessons from Nepal

Nr. 82 – 2020 Vu Le Tran
Expected Returns: An Empirical Asset Pricing Study

Nr. 83 – 2020 Marit Breivik-Meyer
It takes two to tango:
The role of incubators in the early development of start-ups

Nr. 84 – 2021 Per Ivar Seljeseth
Assessing Outcomes from Business-to-Business Selling

Nr. 85 – 2021 Amsale Kassahun Temesgen
Human Wellbeing and Local-level Sustainability

Nr. 86 – 2021 Ensieh Roud
The Role of Joint Training in Inter-organizational Collaboration in Emergency Management

Nr. 87 – 2021 Menghan Yuan
Climate Change and Economic Growth: An Empirical Study of Economic Impacts of Climate Change

Nr. 88 – 2021 Saiful Hasan
Electric Vehicle Adoption: Empirical Analyses

Nr. 89 – 2021 Irina Nikolayevna Isaeva
Managing multiple goals in university-industry collaboration

Nr. 90 – 2022 Yevheniia Antoniuk
Impact of climate change risks on the financial markets

Nr. 91 – 2022 Oliver Henk
One-size-fits-all? The role of internal control for identifying and mitigating risks of interorganizational relationships

Nr. 92 – 2022 Iselin Kristine Mauseth Steira
Learning Takes Teamwork – the Role of New Venture Teams in Entrepreneurship Education

Nr. 93 – 2022 Lidia Kritskaya
Hybrid Entrepreneurship and Staged Entry into Self- employment

Nr. 94 – 2022 Silje Aakre
From intangibility to 'fluid' tangibility of cyberrisk: localisation, visualisation, and prevention

In a digitalised and globalised world, cyberrisk has become a key concern for organisations. The challenge is that global cyberrisk is intangible – almost like gas – something that cannot be discerned in the traditional way, but which can cause fatal consequences. To avoid being trapped in a paralysed state of unknowing, we need theory to interpret cyberrisk, and perspectives to intervene with the intangibility. This dissertation applies Beck's risk society thesis, and asks: *what challenges does the intangibility of cyberrisk represent for organisations, and how can they mitigate the intangibility of cyberrisk?*

The intangibility of cyberrisk is studied by applying Giddens' understanding of manufactured risks, and by extending Beck's typology and features of global manufactured risks in the risk society. The dissertation argues that cyberrisk is the archetype of global risks, and therefore by its very nature, intangible. Four perspectives on cyberrisk are studied in the incorporated articles addressing regulations, openness, foresight, and strategy. These four perspectives allow us to intervene with intangibility. Cyberrisk can be *localised* by approaches to assess its manifested and imagined consequences. It can be *visualised* to allow for a more meaningful discussion of cyberrisk, and consequently, *prevented*. This way, cyberrisk no longer remains in a gas state, but can become 'fluid' and thus, more tangible allowing for mitigation.

In addition to the individual contributions of research articles incorporated into this dissertation, the overarching discussions synthesizing them as a whole makes contributions to the (world) risk society thesis. It achieves this by extending Beck's typology of global risks and elaborating on the role and magnitude of cyberrisk in the risk society. Finally, this dissertation highlights the intangibility of cyberrisk in a managerial context and suggests perspectives and strategies to interpret and mitigate intangible cyberrisk.

NORD University

ISBN: 978-82-92893-84-5
ISSN: 2464-4331
Trykk: Trykkeriet, Nord universitet
www.nord.no