NTNU
Norwegian University of
Science and Technology

The Norwegian Downsizing Approach in Terms of the Insider Threat

An interpretive study

Terje Benjaminsen

Master in Information Security
Submission date: June 2017
Supervisor: Stewart Kowalski, IIK
Co-supervisor: Ronny Windvik, Norwegian Defence Research Establishment (FFI)

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

Preface

This thesis completes a two-year study program in Master of Information Security (MIS) at NTNU. The study was carried out as independent work during the spring semester of 2017. In addition to the internal supervisor at NTNU, Norwegian Defence Research Establishment (FFI) supported me with a co-supervisor.

The idea for this thesis started as conversations with Steffen Olsen, a friend and MTM NTNU alumni, with common interests in the field of security management. We discussed various aspects of the insider threat in general terms. After some meetings with my supervisors, we agreed on focusing on how Norwegian enterprises approach a downsizing in terms of the insider threat.

The reader of this thesis should be familiar with basic terms concerning organizational change and security management. Deeper understanding within topics such as personnel security and risk management will be helpful, yet not mandatory, in order to grasp the context. The target reader might be part of top management, security management, or human resources in large Norwegian enterprises.

01-06-2017

Acknowledgments

I would like to thank my supervisors, Stewart Kowalski and Ronny Windvik, for their steady guidance and support. I have learned a great deal about research in general, and security management in particular.

I would also like to thank my employer for their support, and opportunity to complete this master's degree. Thanks also to the Norwegian Defence Research Establishment (FFI) for all the support and providing the co-supervisor.

I thank my interviewees for their openness and knowledge. It certainly takes some courage sharing your opinions with an outsider, while discussing the insider threat. Thanks also to my network for introducing me to these experts.

Thank you, Jon Everett, for your constructive and detailed feedback in the final stage of proof-reading.

Finally, a special thanks to my family for all their patience and love during this challenge. Marte, I could not have done this without your support. Benjamin and Adrian, I will clear the desk in your room for books on research and security management. Now you have a desk for doing your homework.

T.B.

Abstract

Many Norwegian enterprises in various sectors have been downsizing over the last decade. Among the current threats to organizations, the insider threat could be the most significant. This threat might be increased during or after a downsizing process.

This research examined how the Norwegian organizations approach a downsizing in terms of the insider threat. Ten subject matter experts in large Norwegian enterprises were interviewed. These subject matter experts serve in various industry sectors such as; petroleum and energy, climate and environment, agriculture and food, defense, finance, and maritime. The size of the organizations varies from around 400 to more than 10,000 employees. The results of these interviews have been discussed and partially compared with international practice. Then, authorities within the field of security management have commented on the findings and the suggested improvements. This is a qualitative study that describes and interprets the Norwegian approach, which provides strong rights for the employees, and does not examine cause and effect relationships.

The analysis has identified management as a key element to mitigate the insider threat in downsizing processes. Starting with top management in the planning phase, then transferring more responsibility on the middle management in the execution phase. Managers might not be aware of having such responsibility concerning the insider threat. The managers are additionally key players in building a healthy security culture. Given this important role, there seem to be a surprisingly low level of education and training aimed at personnel security management. Additionally, one must consider both the dismissed and the remaining employees. As a foundation, enterprises should have established policies, procedures, and holistic risk management, including the insider threat. Further, some enterprises could transform their approach from reactive towards proactive, and mitigate the insider threat by combined social and technical controls throughout the employment lifecycle. However, with adherence to rules and regulations, such as the EU General Data Protection Regulation (GDPR) concerning privacy.

Neither the Norwegian National Security Authority (NSM), the Norwegian Center for Information Security (NorSIS), or the Norwegian Business and Industry Security Council (NSR), with their background and expertise, question the findings.

To the authors knowledge, there have not been similar previous research, on how Norwegian organizations approach a downsizing in terms of the insider threat.

Sammendrag

Mange norske bedrifter i ulike sektorer har nedbemannet i løpet av det siste tiåret. Blant de nåværende truslene mot organisasjoner, kan innsidetrusselen være den viktigste. Denne trusselen kan økes under eller etter en nedbemanningsprosess.

Denne studien har forsket på hvordan norske organisasjoner tilnærmer seg en nedbemanningsprosess med tanke på innsidetrusselen. Ti fageksperter i store norske bedrifter ble intervjuet. Disse fagekspertene tilhører ulike industrisektorer som; olje og energi, klima og miljø, landbruk og mat, forsvar, finans og maritimt. Størrelsen på organisasjonene varierer fra rundt 400 til over 10.000 ansatte. Resultatene av disse intervjuene er blitt diskutert og delvis sammenlignet med internasjonal praksis. Deretter har autoriteter innen sikkerhetsstyring kommentert funnene og de foreslåtte forbedringene. Dette er en kvalitativ studie som beskriver og tolker den norske tilnærmingen, som gir sterke rettigheter til de ansatte, og undersøker ikke årsakssammenhenger.

Analysen har identifisert ledelsen som et sentralt element for å redusere innsidetrusselen i nedbemanningsprosesser. Det starter med toppledelsen i planleggingsfasen, hvor det overføres mer ansvar på mellomledelsen i utførelsesfasen. Lederne er kanskje ikke er klar over at de kan ha et slikt ansvar med tanke på innsidetrusselen. Gitt denne viktige rollen er det overraskende lite utdanning og opplæring rettet mot personellsikkerhetsstyring. Man må vurdere både de oppsagte og gjenværende ansatte, under og etter en nedbemanningsprosess. Som et utgangspunkt må noen bedrifter starte med å etablere retningslinjer, prosedyrer, og helhetlige risikostyring, som inkluderer innsidetrusselen. Noen bør endre sin tilnærming fra reaktiv mot proaktiv, samt håndtere innsidetrusselen ved kombinerte sosiale og tekniske tiltak gjennom hele ansettelsesløpet. Dette må selvsagt sees i sammenheng med lover og regler, slik som den nye personvernforordringen.

Hverken Nasjonal sikkerhetsmyndighet (NSM), Norsk senter for informasjonssikring (NorSIS) eller Næringslivets Sikkerhetsråd (NSR), med sin bakgrunn og kompetanse, betviler studiens funn.

Til forfatterens kunnskap har det ikke vært lignende tidligere forskning om hvordan norske organisasjoner tilnærmer seg en nedbemanningsprosess med tanke på innsidetrusselen.

Contents

List of Figures

List of Tables

1 Introduction

1.1 Topics Covered

"*Insider attacks are a well-known problem acknowledged as a threat as early as 1980s*" [1]. Standards Norway (SN) defines risk in terms of threat, vulnerability, and asset [2]. This thesis will focus on the threat dimension, more accurately the insider threat while downsizing. Management at all levels will be a key element throughout the thesis. Other topics include; whistleblowing versus insider attack, privacy, social and technical controls, disgruntlement, risk assessment, and security culture.

1.1.1 Definitions

- **Insider**: "*An insider is a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization's structure*" [3].
- **Threat**: "*A threat is an undesirable negative impact on your assets*" [4].
- **Insider threat**: "*The insider threat is the threat that the insider may abuse her discretion by taking actions that would violate the security policy when such actions are not warranted*" [5].
- **Organization change**: "*Company or organization going through a transformation. Organization change occurs when business strategies or major sections of an organization are altered*" [6].
- **Downsizing**: "*Intentional action aimed at reducing the workforce with a view to improving the efficiency or effectiveness of the organization*" [7, 8].
- **Disgruntlement**: *Employee observed to be dissatisfied in current position; chronic indications of discontent, such as strong negative feelings about being passed over for a promotion or being underpaid, undervalued; may have a poor fit with current job* [9].

1.2 Keywords

Management, insider threat, personnel security, downsizing, qualitative research, grounded theory.

1.3 Problem Description

Many Norwegian enterprises in various sectors have been downsizing over the last decade. Among the current threats to organizations, the insider threat might be significant. This threat could be increased during or after a downsizing process.

Information security experts around the world seem to disagree on how significant the insider threat actually is. IBM [10] and Information Security Forum (ISF)[11] claim that insiders pose as the most significant threat to organizations in 2016. "*ISF suggests three types of risk behavior of insiders; malicious, negligent, and accidental*" [11]. IBM claims that 44,5% of all attacks reported in 2015 were by malicious insiders [10], while ISF claims that the vast majority of insider incidents were a result of accidental or inadvertent behavior [11]. A survey among Norwegian companies disclosed that 28% have revealed a malicious insider activity, and that merely 38% of these companies pressed charges [12].

In today's dynamic society it is normal to switch jobs on occasion. A research by Carnegie Mellon suggest that a specific event or series of events triggered the insider attack in 92% of the cases they examined [13]. "*These events included, among others, various work-related events to include employment termination (47%), dispute with a current or former employer (20%), and employment related demotion or transfer (13%)*" [13]. Additionally, in similar research they claim that 32% of the insiders were perceived by colleagues as disgruntled employees [14]. This might provide an employee with both the motive and opportunity to launch an insider attack. Elmrabit et al. suggest motive, opportunity, and capability, as psychological indicators for malicious insiders [15]. "*Motivation will come from internal, personal drivers, whereas opportunity and capability will be given to insiders overtly by your organization*" [16].

Why do people decide to violate company security policy, and become a malicious insider, or even a criminal? According to Hirschi's social learning theory, "*a person becomes a criminal due to sociological influences wherein he/she learns to be a criminal*" [17]. This theory may also apply to the violation of company policy, hence the insider threat. A more proactive approach is suggested by Clarke in his situational crime prevention theory, suggesting that it is best to prevent the crime from happening in the first place [17, 18].

There is likely no technical solution to the problem, and Keeney et al. (2005) suggest that "*management attention is needed for employees who experience negative work-related events*" [13]. According to Saathoff et al. (2013) one must pay attention to the underlying behavioral components of the insider threat, and implement sufficient security controls [19]. To the authors knowledge, there is no research on the insider threat while downsizing in Norwegian organizations.

1.4 Justification, Motivation and Benefits

As described in the problem description, the insider threat is a real problem. Organizational change is a continuous process, resulting in employees that on occasion will lose their jobs, and may pose as an insider threat. Norway seems to have strong employee rights and very long notice time compared to e.g. the United States. Stakeholders in Norwegian enterprises might benefit from both the international best practice as described in Chapter 2, and the derived theory in Chapter 5 on how to approach a downsizing in terms of the insider threat.

1.5 Research Questions

1. How do Norwegian organizations approach a downsizing in terms of the insider threat?
2. How can the insider threat on dismissals be reduced through improved downsizing processes?

1.6 Planned Contributions

This thesis should review how relevant literature approach the research problem in general, how Norwegian organizations approach it in practice, and ultimately suggest improvements. This is achieved through interviews, which are analyzed and discussed in order to develop a theory.

1.7 Limitations

I only interviewed large Norwegian organizations that were available through 1st, 2nd, and 3rd order contacts in my network. The time frame for the interviews was also limited to a few weeks, which resulted in me having to decline two additional interviewees. This kind of independent qualitative research depend a great deal on the researcher's experience, knowledge, and network. I conducted the interviews and coding in Norwegian, before analyzing and discussing the results in English. Some interviewees had limited knowledge in their organization's policies and procedures concerning organizational change. Nevertheless, this provided an alternative perspective and added value to the results. It could have been a limitation to the research while only conducting ten interviews. However, during the interviews the key findings was repeated in various forms, and it is not likely that more interviews would change this significantly.

1.8 Structure of the Thesis

This thesis starts by describing relevant work and background information in Chapter 2, providing sufficient context prior to reading the results and discussion chapters. In Chapter 3 I describe the choice of methods for my study, while Chapter 4 presents the results from my interviews. The findings are discussed in Chapter 5, followed by a quality assurance by security experts and authorities in Chapter 6. Finally, I conclude in Chapter 7, and suggest further work in Chapter 8.

2 Background

This chapter will describe relevant work and background information, providing sufficient context prior to reading the results and discussion chapters. International practices and organizational change in general will be described in order to see the broader picture, despite the focus is on Norwegian conditions in downsizing processes. The first research question focus on how Norwegian organizations approach a downsizing in terms of the insider threat. This question has been split up in three parts in order to pin point related sources to specific topics, and explain how these sources might provide answers. The three parts are (I) *organizational change frameworks*, (II) *personnel security*, and (III) *layoff process*. The second research question focus on improvements.

The background chapter has been developed in several stages. First a broad literature review, in order to gain sufficient knowledge, then continuously improved throughout the research process. This chapter is structured similar to the discussion chapter, which is structured under the main sections; plan, do, check, and act.

2.1 Organizational Change Frameworks

In this section I will describe relevant sources concerning organizational change frameworks. The sources include Norwegian rules, legislation and regulations, various guidelines, as well as some change models.

2.1.1 Rules and Regulations

An organizational change might be invoked by downsizing, merger, or outsourcing. According to the Norwegian Working Environment Act, "*the employer shall ensure the necessary information, participation and competence development to meet the requirements of this Act regarding a fully satisfactory working environment*" [20, 21]. Additionally, in such change processes, the Act states that a risk assessment is mandatory in order to reduce the uncertainty among the employees. In Norway, mass dismissals are regulated through the Working Environment Act, and become operative when a minimum of ten employees are laid off within a period of 30 days [7].

In addition to the Working Environment Act, the various unions have their so called Basic Agreements (HTA) with organizations for employers [22, 23, 24]. The government claims that fair co-determination according to the Basic Agreement yield the most successful processes and results [23]. The Basic Agreement between

The Confederation of Norwegian Enterprise (NHO) and The Norwegian Confederation of Trade Unions (LO) states that the management shall discuss employment matters, including reduction plans, with the shop stewards as early as possible [24]. Similar basic agreements between other employer unions and employee unions exists.

2.1.2 Guidelines

The Ministry of Local Government and Modernisation (KMD) have issued a personnel policy on organizational change procedures [25]. This policy addresses the responsibilities of senior executive, relationship to the employees, and the role of middle management during such process. As an example, Troms fylkeskommune has developed a guideline for organizational change [26], which includes check lists concerning risk assessment [27] and downsizing [26]. However, this risk assessment does not consider the insider threat.

2.1.3 Change Models

This thesis will not argue strengths and weaknesses of change models. However, this section will show four change models of various complexity. The four models are; Lewin's three-stage process for planned change [28, 29], Kolb and Frohman's model of the consulting process [30], Koter's 8-Step Process for leading change [31, 29], Kolb and Frohman's model of the consulting process [30], and Hoshin Kanri [32].

Lewin's Three Stage Process

The Lewin's three stage process for planned changes includes; (1) unfreezing, (2) changing, and (3) refreezing [28, 29, 30]. It was developed during the 1950s [29]. In the first stage you have to unfreeze the organization, motivating it for changing. Then you do the actual change, before refreezing and making the changes stick. This is a simple model and is "*characterized by rational thinking and change optimism*" [29].

Kolb and Frohman's Model

Keen (1981) claims that the Kolb and Frohman's model of the consulting process is an extension of the Lewin process as described above [30]. Kolb and Frohman's model includes; (1) scouting, (2) entry, (3) diagnosis, (4) planning, (5) action, (6) evaluation, and (7) termination. Keen claims that step 1-2 relate to unfreezing, step 3-5 relate to changing, while step 6-7 relate to refreezing.

Kotter's 8-step Process

A more recent model, the Kotter's 8-step process for leading changes, includes; (1) *create* a sense of urgency, (2) *build* a guiding coalition, (3) *form* a strategic vision & initiatives, (4) *enlist* a volunteer army, (5) *enable* action by removing barriers, (6) *generate* short-term wins, (7) *sustain* acceleration, and (8) *institute* change [33, 31, 29]. This model is aimed more at the managers and how to lead the process, while the employees simply have to survive the change [29].

Hoshin Kanri

Hoshin Kanri is a four step change process, based on the Plan-Do-Study-Act model [32], also known as Plan-Do-Check-Act (PDCA)cycle. The discussion in Chapter 5 is structured according to the PDCA cycle. The Hoshin Kanri change process consists of the four steps; (1) Mission vs Strategies, (2) Strategies vs Objectives, (3) Objectives vs Goals, and (4) Goals vs Team Actions. This process aims at continuous improvements, inclusion, creativity and innovation. It involves all levels in the organization, from top management, via middle managers, to team members.

Comparing Change Models

The above described change models are shown and compared in Table 1. The table is an expansion of a similar table by Keen (1981), comparing Lewin's process with Kolb and Frohman's model [30]. Keen (1981) uses the Lewin process in addition to Kolb and Frohman's model of the consulting process, in order to describe a tactical approach to overcome social inertia in organizational change processes [30]. "*'Social inertia' is a complicated way of saying that no matter how hard you try, nothing seems to happen*" [30].

Lewin	**Kolb & Frohman**	**Kotter**	**Hoshin Kanri**
Unfreezing	Scouting Entry	Create Build Form	Mission/Strategies
Changing	Diagnosis Planning Action	Enlist Enable Generate Sustain	Strategies/Objectives
Refreezing	Evaluation Termination	Institute	Objectives/Goals Goals/Team Actions

Table 1: Comparing change models

2.1.4 Successful Change Process

Saksvik et al. (2008) claim that managers who share information with the employees, values the employees and thereby promote trust, and fair communication [34]. Rørvik and Nesheim (2010) claim that heaps of information, great openness, and good communication, were criteria for success during downsizing and restructuring [7]. They additionally claim that the union could provide the management with employee's experiences and reactions to the downsizing measures. Measures concerning the insider threat might be implemented in all stages of such change processes.

2.2 Layoff Process

In this section I will describe relevant sources concerning the layoff process. Layoff notices might be issued during downsizing, mergers or outsourcing. Causes for layoffs could include, but are not limited to, cutting cost in difficult times, or termination of redundant or irrelevant resources. Freeman and Cameron (1993) have defined downsizing as "*intentional action aimed at reducing the workforce with a view to improving the efficiency or effectiveness of the organization*" [7, 8].

Whitman and Mattord (2011) suggest different aspects while downsizing, including access control, hostile and friendly departure, and exit interview [35]. Whitman and Mattord (2011) suggest performing the following tasks when an employee prepares to leave the organization [35]:

- Access to the organization's systems must be disabled.
- Removable media must be returned.
- File cabinet locks must be changed.
- Office door lock must be changed.
- Keycard access must be revoked.
- Personal effects must be removed from the organization's premises.

After these tasks have been conducted, organizations often use an exit interview, reminding on potential obligations, before escorting the employee from the premises [35]. Whitman and Mattord (2011) consider a downsizing as a hostile departure, and suggest revoking access before the employee has a chance to exploit it. In contrast to this, the Norwegian Working Environment Act chapter 15, states the termination of employment relationships, including periods of notice and multiple variants of protection against dismissal [20]. E.g. Basic Agreements states at least 14 days notice, when issuing collective notice of stoppage (often during industrial disputes) [22, 23, 24].

According to Rørvik and Nesheim (2010), the arrangement with severance pay has evolved outside the Norwegian legislation, resulting in a transformation from downsizing regulated by law toward norm based downsizing [7].

2.2.1 Psychosocial Consequences

Downsizing processes have a psychosocial aspect as well, , both for the remaining employees and those who are dismissed. Relevant literature and research indicate that it is not merely *that* the downsizing process occurs, rather *how* it is conducted, that affects the employee's motivation [36, 37]. In other words, the employee's perception of the change process might yield psychosocial consequences, and influence their motivation for launching an insider attack.

The Dismissed

Possible negative effects on the dismissed includes i.e. failed health, financial difficulties, alcohol-related diseases, and grief reaction possibly resulting in depression [38]. In a recent PhD thesis, Reiso suggests the "*scarring effects of early-career unemployment*" [39]. The National Institute of Occupational Health (STAMI) issued a fact-book on occupational health and safety in 2015 [40]. This fact-book describes negative impacts of downsizing and unemployment, and suggests a "*clear correlation between unemployment and the development of depression*". Further, they refer to studies indicating health benefits of getting back to work, provided it is a good and safe job. According to STAMI, Norwegian studies claim that downsizing increase the risk of disability, general mortality, and mortality due to cardiovascular disease. Such psycho-social reactions might be related to the insider threat while downsizing. Both for the dismissed and the remaining employees.

Survivor Syndrome

The term ’survivor syndrome’ is indicating the negative effects on job satisfaction and motivation [36], in addition to emotions and reactions survivors might experience during downsizing [41]. Such negative effects could include; insufficient attention towards the ’survivors’ in a downsizing, negative emotions as e result of losing colleagues, or decreased capacity among the ’survivors’. Thus, measures during and after a downsizing should not only be aimed at the dismissed. The survivors might deserve special attention as well.

2.3 Personnel Security

In this section I will describe relevant sources concerning personnel security and the insider threat. This includes; definitions of the insider threat, Norwegian conditions, the dilemma between whistleblowing and insider threat, trust and loyalty, privacy, and aspects from criminology.

To the authors knowledge, available Norwegian organizational change frameworks does not consider the possible insider threat. The 'Data Breach Investigations Report' (2016) claims that privilege abuse is the top misuse action of insiders, and that the "*actions of insiders are among the most difficult to detect*" [42].

2.3.1 Defining the Insider Threat

It is difficult to define security. In terms of this thesis, security has been divided into the three areas; physical security, personnel security, and information security. Further, the insider threat aligns with personnel security. This is similar to how the Centre for the Protecting of National Infrastructure (CPNI) in UK [43] and the Norwegian Security Act [44], and NSM [45], divides categories of security as well.

This section will show various definitions of the insider threat and personnel security by Bishop, Carnegie Mellon University, and CPNI.

Bishop

Bishop has published articles on the insider threat [46, 47], and co-edited the book 'Insider Threats in Cyber Security' [3]. Bishop defines the insider threat as follows [5]:

> *The insider threat is the threat that the insider may abuse her discretion by taking actions that would violate the security policy when such actions are not warranted.*

Carnegie Mellon University's Software Engineering Institute

Carnegie Mellon University's Software Engineering Institute has published studies concerning the insider threat in various sectors [48, 14, 13, 49], and suggests the following definition of a malicious insider [50]:

> *A malicious insider is defined as a current or former employee, contractor, or business partner who meets the following criteria:*
>
> - *has or had authorized access to an organization's network, system, or data.*
> - *has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.*

CPNI

"*CPNI is the government authority for protective security advice to the UK national infrastructure*" [51]. CPNI describes personnel security as follows [52]:

> *Personnel security is a system of policies and procedures that seek to manage the risk of people exploiting, or having the intention to exploit, their legitimate access*

> *to an organization’s assets for unauthorized purposes. Those who seek to exploit their legitimate access are termed ’insiders’.*

Further, CPNI describes three main types of insider behavior [53]:

> ***Deliberate insider:*** *those who obtain employment with the deliberate intent of abusing their access.*
> ***Volunteer/self-initiated insider:*** *those who obtain employment without deliberate intent to abuse their access but at some point personally decide to do so.*
> ***Exploited/recruited insider:*** *those who obtain employment without deliberate intent to abuse their access but at some point are exploited or recruited by a third party to do so.*

The latter two are defined as *opportunistic*, and the findings from a CPNI study suggest that 76% of the cases were self-initiated [53]. In the same study, the primary motivation for insider activity was financial gain (47%), ideology (20%), desire for recognition (14%), loyalty to friends/family/country (14%), and revenge (6%).

NSM
"*The Norwegian National Security Authority (NSM) is a cross-sectoral professional and supervisory authority within the protective security services in Norway*" [54]. NSM defines personnel security as follows [45]:

> *Personnel security is about ensuring that personnel and employees have a behavior that does not compromise information or objects; in short, the employees are trusted.*

Summary Defining the Insider Threat

The definitions on the insider threat differ somewhat concerning both scope and intent. Bishop has a broad view, including both the intended and unintended actions, in addition to referring to violation of the security policy in general. While, Carnegie Mellon focus on the intended actions of both current and former authorized individuals, targeting information and information systems. CPNI focus on the intentional insiders, and includes all the organization’s assets, hence not only computer systems. In Norway, NSM focus on trust in the employees, protecting both information and physical objects.

2.3.2 Norwegian Conditions

Syvertsen (2007) published his master thesis elaborating on the insider threat in Norway, compared to the US [55]. This was a quantitative study with a survey sent out to 50 companies, whereof only 7 responded. Based on this, Syvertsen (2007) did not reach a final conclusion concerning the insider threat in Norway, though none of the respondents reported such incidents. Nevertheless, in terms of Norwegian research related to my study, Syvertsen’s work seems to be most relevant one.

More recently, The Norwegian Business and Industry Security Council (NSR) have performed surveys concerning criminality and security since 2006, and claims that 28% of the participating Norwegian companies revealed a malicious insider, and that merely 38% of these companies pressed charges [12].

NSM published their security professional advice in 2015 [45]. In this report, NSM claims that the insider showed signs prior to the incident, of being or becoming a malicious insider. Further, NSM claim that more education concerning security tasks are required, both in public and private sector.

2.3.3 Whistleblowing or Insider Attack?

Another aspect is whether the disclosure of business confidential information or government classified information, is the act of a whistle blower, or the act of a malicious insider. The Norwegian Working Environment Act section 2-4, states that "*an employee has a right to notify concerning censurable conditions at the undertaking*" [20]. On the other hand, the Norwegian Security Act section 12 states the "*duty to protect classified information*" [44]. Additionally, in organizations not compliant to the security act, employees often have to sign a non-disclosure agreement.

2.3.4 Trust and Loyalty

Downsizing might be perceived as a violation to the ’psychological contract’ between an organization and the employees, resulting in broken trust and increased level of stress [7]. A skewed balance in this ’psychological contract’ might provide negative effects such as distrust, as well as reduced loyalty and organizational affiliation [7]. Trust and loyalty is also an issue concerning whistleblowing.

2.3.5 Privacy

The Norwegian Labour Inspection Authority, The Norwegian Data Protection Authority, The Petroleum Safety Authority Norway, and the social partners, developed guidelines for control and surveillance in employment [56]. According to this guideline, controls and surveillance are regulated by two legislations; the Working Environment Act and the Personal Data Act [56]. The latter will be replaced by the EU General Data Protection Regulation (GDPR) [57] in 2018. According to the Norwegian Ministry of Justice and Public Security, the GDPR will continue the key principles and rules of current Norwegian Personal Data Act, as well as contribute to a more harmonized regulatory framework in Europe [58]. Controls and data processing must be interpreted and practiced in terms of each other, and the enterprise’s benefits of a measure must out-weigh the negative effects it has on the employees. [56]. Thus, privacy must be considered while implementing controls in order to mitigate the insider threat.

2.3.6 Criminology

Why do people decide to violate company security policy, and become a malicious insider, or even a criminal? This is not the core of this thesis, nevertheless it deserves some attention. Crime theories have been used in order to improve information security techniques and controls [59]. This section will describe some relevant crime theories that might help in mitigating the insider threat.

Edwin H. Sutherland developed his differential association theory, published in 1949 [60]. It suggests that "*criminal behavior is learned in association with those who define such behavior favorably*" [60]. Martinko et al. developed the causal reasoning theory, "*proposing that individuals' attributions about the causal dimensions of workplace events are a primary factor motivating both the emotions and behaviors that result in counterproductive workplace behaviors*" [61, 62]. According to Hirschi's social learning theory, "*a person becomes a criminal due to sociological influences wherein he/she learns to be a criminal*" [17]. Or, that *influence of peer behavior encourages a person to do certain things under pressure, which they would not do otherwise* [63]. This theory has similarities with the art of social engineering. *Social engineering is the act of manipulating a person to take an action that may or may not be in the "target's" best interest* [64]. The rational choice theory claims that, "*if the perceived benefits from committing the crime outweigh the costs, both examined probabilistically, then one will decide to commit the crime*" [17]. Thus, it is a cost vs benefit decision. Clarke's situational crime prevention theory suggests that it is better to prevent the crime, rather than detecting it afterwards [18, 17]. The general deterrence theory "*is based on the hypothesis that people make logical decisions based on the maximization of their benefit and the minimization of cost*" [65]. Hence, deterrent actions should be able to influence behavior and criminal intentions [63]. The theory of planned behavior attempts to explain the causal relation underlying human behavior [65]. Assuming that a person's behavior might be predicted based on his/her intentions [65], or "*perceived behavioral control*" [63]. The theory of anomie may be used in order to understand deviant behavior, and motivations for such behavior might be a result of rapid technological changes [63].

Applying Crime Theories in Security Management

Theoharidou et al. (2005) compared crime theories against the effectiveness of ISO17799 (renamed as ISO27002 in 2007) [65]. Coles-Kemp and Theoharidou seem to have further developed this approach, claming that "*crime theories can contribute additional security management techniques and controls*" [59]. Mishra and Dhillon (2006) investigated information security governance from a behavioral perspective, providing the theory of anomie to understand deviant behavior [63].

2.4 Personnel Security Maturity Model

In this section I will describe three maturity models; CPNI's Personnel Security Maturity Model (PSMM) [66], NSM's maturity level for security management [67], and CMMI Institute's Capability Maturity Model Integration (CMMI) [68]. These models ranges from level 1 to level 5, where level 1 is low maturity, and level 5 is high maturity. Each level of the three models are given descriptive names, as shown in Table 2.

Level	**NSM**	**CPNI**	**CMMI**
1	Occasional	Innocent	Initial
2	Fragmented	Developing	Managed
3	Formalized	Competent	Defined
4	Systematized	Effective	Quantitatively managed
5	Optimized	Excellent	Optimizing

Table 2: Comparing maturity models

The three models have various ways of defining each level of maturity. Phrases used in the three models include:

- **Level 1**
  - Firefighting. No formal personnel security policies, training or procedures. Unpredictable and reactive.
- **Level 2**
  - Partial and divided. Undefined responsibilities between operations and audit. Some documentation. Managed on the project level.
- **Level 3**
  - Management attention. Roles and responsibilities defined. There is an organization wide consistent approach to security with defined processes in place. Proactive.
- **Level 4**
  - Risk management. Competence in enterprise. The Executive board recognizes that security is important. Measured and controlled.
- **Level 5**
  - Continuous improvements and development. The prevention of Personnel Security incidents is a core company value, and a board level member of staff has overall responsibility for Personnel Security. The Personnel Security risk assessment is reviewed at least once a year.

Based on the maturity models described above, a simple Personnel Security Maturity Model (PSMM), as shown in Figure 1, has been developed. As this model is developed while discussing the results, it should not strictly be a part of this chapter. However, this model is central in measuring the maturity level of the participating enterprises, and will provide relevant context to the reader throughout this thesis. Hence, the model is also included here.

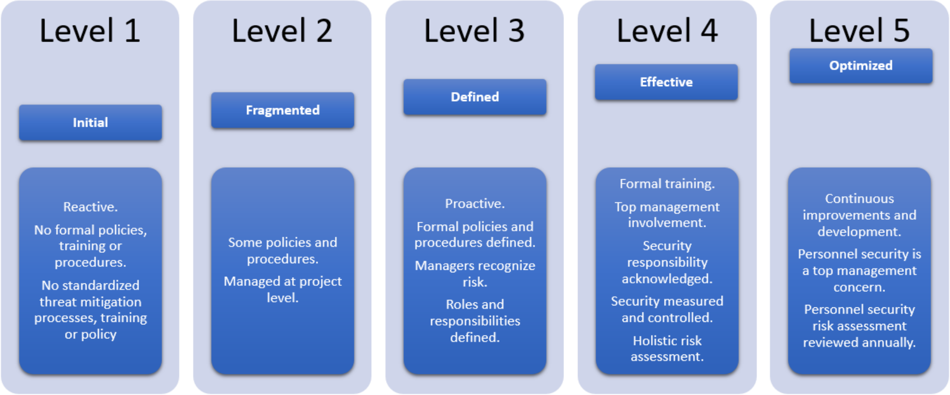
Level 1
Initial
Reactive.
No formal policies, training or procedures.
No standardized threat mitigation processes, training or policy
Level 2
Fragmented
Some policies and procedures.
Managed at project level.
Level 3
Defined
Proactive.
Formal policies and procedures defined.
Managers recognize risk.
Roles and responsibilities defined.
Level 4
Effective
Formal training.
Top management involvement.
Security responsibility acknowledged.
Security measured and controlled.
Holistic risk assessment.
Level 5
Optimized
Continuous improvements and development.
Personnel security is a top management concern.
Personnel security risk assessment reviewed annually.

Figure 1: Personnel Security Maturity Model

2.5 Existing Best Practices

This section will focus on research question two, and literature which support improvements in downsizing processes in terms of the insider threat.

The Ministry of Defence received an Official Norwegian Report in 2016 (NOU 2016:19), which proposed a new Security Act [69]. This report suggests that the new Security Act should facilitate efficient prevention against and detection of malicious insiders accessing information or areas of critical impact. Carnegie Mellon University and affiliated experts, have suggested various measures for mitigating the insider threat. Some suggest system dynamic approaches to simulate and map the insider threat [70, 71]. This provides the opportunity to "*understand, characterize, and communicate the impact of a malicious threat environment on organizational and system operations and their respective missions*" [72]. The book 'Insider Threats in Cyber Security' [3] is a collection of articles describing the insider threat, and suggested approaches for combating and mitigating this threat. Legg et al. (2013) suggest a "*conceptual model for insider threat and a reasoning structure that allows an analyst to make or draw hypotheses regarding a potential insider threat based on measurable states from real-world observations*" [73]. While, Sokolowski and

Banks (2016) describes "*an agent based approach to model the insider threat*" [74]. Chabinsky (2014) claims that "*a successful insider threat program must include active participation from a company's physical security, personnel security, information technology, human resources and procurement/ sourcing staff*" [75].

Carnegie Mellon University (2012) suggests 19 best practices in their *Common Sense Guide to Mitigating Insider Threats* [50]:

1. Consider threats from insiders and business partners in enterprise-wide risk assessments.
2. Clearly document and consistently enforce policies and controls.
3. Incorporate insider threat awareness into periodic security training for all employees.
4. Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
5. Anticipate and manage negative issues in the work environment.
6. Know your assets.
7. Implement strict password and account management policies and practices.
8. Enforce separation of duties and least privilege.
9. Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
10. Institute stringent access controls and monitoring policies on privileged users.
11. Institutionalize system change controls.
12. Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.
13. Monitor and control remote access from all end points, including mobile devices.
14. Develop a comprehensive employee termination procedure.
15. Implement secure backup and recovery processes.
16. Develop a formalized insider threat program.
17. Establish a baseline of normal network device behavior.
18. Be especially vigilant regarding social media.
19. Close the doors to unauthorized data exfiltration.

2.5.1 Indicators

Indicators might help us to detect and understand insider activity. Costa et al. (2016) suggest an ontology for insider threat indicators [76], in order to ensure increased awareness. "*The end goal is for organizations that use the ontology to be able to communicate indicators of insider threat consistently and without revealing sensitive information*" [76].

Greitzer et al. (2012) suggest 12 psychosocial risk indicators; disgruntlement, difficulty accepting feedback, anger management issues, disengagement, disregard for authority, performance, stress, confrontational behavior, personal issues, self-centeredness, lack of dependability, and absenteeism [9]. Their definition of disgruntled is shown in the beginning of Chapter 1.

2.5.2 Social and Technical Controls

Technical controls might include physical access control, information systems access control, intrusion detection and prevention systems (IDPS). While, social controls could include background and identity check, detection of behavioral change, and authorization conversation.

According to Saathoff et al. (2013), technical controls are not sufficient [19, 77]. This is supported by Harkins (2016) who claims that, "*we have a tendency to overlook the people factor in technical organizations, and rather focus on the technical challenges*" [78, 79]. Kowalski (1994) integrates the Steinmetz victimological Risk Analysis model into the security by consensus (SBC) model, suggesting a relationship between the crime types and the crime prevention measures [80, 81]. In other words, technical controls to mitigate technical problems, and social controls to mitigate social problems. One should pay attention to the environment and the underlying behavioral components of the insider threat [19, 77]. Additionally, Gubbi et al. (2013) state that encryption will not protect against an insider who launches a malicious attack [82, 77]. Andersen et al. (2004) claim that:

> *Organizations should focus on intrusion detection and response holistically by integrating a comprehensive intrusion detection and response capability with an organization's policies and procedures, as well as with the technology* [71].

Access controls seem to be basic measures in order to ensure confidentiality in terms of information security. Whitman and Mattord (2011) suggest a set of 20 access controls [35]:

1. Access Control Policy and Procedures.
2. Account Management.
3. Account Enforcement.
4. Information Flow Enforcement.
5. Separation of Duties.
6. Least Privilege.
7. Unsuccessful Logon Attempts.
8. System Use Notification.
9. Previous Logon Notifications.
10. Concurrent Session Limit.
11. Session Lock.
12. Session Termination.
13. Supervision and Review - Access Control.
14. Permitted Actions without Identification or Authentication.

15. Automated Marking.
16. Automated Labeling.
17. Remote Access.
18. Wireless Access Restrictions.
19. Access Controls for Portable and Mobile Devices.
20. Use of External Information Systems.

The mitigation of a potential insider threat starts prior to employment. The Norwegian Business and Industry Security Council (NSR) has issued guidelines on how to perform a background check [83]. Additionally, a new service has become available recently; the Diploma registry [84]. This solution allows you to "*collect your results from higher education in Norway and share them with potential employers, educational institutions and other relevant recipients*" [84]. According to KRISNO 2015, 34% of the enterprises performed a control of collaborating partners [12]. Further, in private sector 39% performed identity check prior to employment, while the reported share was 48% in public sector. 80% in private sector and 95% in public sector performed reference check, while 29% in private sector and 56% in public sector performed diploma verification.

Social controls might aid the mitigation of the insider threat. Whitman and Mattord (2011) suggest eight personnel security controls [35]:

1. Personnel Security Policy and Procedures.
2. Position Categorization.
3. Personnel Screening.
4. Personnel Termination.
5. Personnel Transfer.
6. Access Agreements.
7. Third-Party Personnel Security.
8. Personnel Sanctions.

Greitzer et al. (2012) developed a psychosocial model "*to assess an employee's behavior associated with an increased risk of insider abuse*" [9]. They suggest predictions using a Bayesian model, combining social and technical indicators in order to enhance situation awareness concerning the insider threat [9]. "*This will transform a reactive/forensics based approach into a proactive one that will help identify employees who are at greater risk of harming the organization or its employees*" [9].

NSM has developed manuals on authorization and authorization conversation, aimed at those compliant to the Security Act [85]. The intentions of this conversation is to assess if the employee should be authorized for accessing classified information. Similar to this, Carnegie Mellon University (2012) suggests "*enforcing separation of duties and least privilege*", and "*institute stringent access controls* *and monitoring policies on privileged users*" [50]. This is echoed by Whitman and Mattord (2011) [35].

2.5.3 Risk Management

Various risk management frameworks and guidelines exist. A holistic risk assessment could include operational risk, physical risk, information security risk, personnel security risk, financial risk, and more. This section will describe one definition of an enterprise risk management (ERM) and one example of a personnel security risk assessment (PSRA) aim.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative that develops frameworks and guidance on enterprise risk management, internal control and fraud deterrence [86]. COSO defines enterprise risk management as follows [87]:

> *Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*

In 2013, CPNI issued a 4th edition of a guideline on personnel security risk assessment [52]. The aim of this guideline is [52]:

> *Personnel security risk assessment focuses on employees, their access to their organization's assets, the risks they could pose and the adequacy of existing countermeasures. This risk assessment is crucial in helping security and human resources (HR) managers, and other people involved in strategic risk decisions, communicate to senior managers the risks to which the organization is exposed.*

Carnegie Mellon University (2012) suggests that enterprises should "*consider threats from insiders and business partners in enterprise-wide risk assessments*" [50].

2.6 Summary of Background

The Literature review have not revealed a comprehensive framework or guidelines that answers my research questions. The sources described in this chapter could have been sufficient in order to develop a best practice in global terms. However, the Norwegian conditions are stricter concerning employee rights and responsibilities. Thus, more information regarding Norwegian downsizing approaches in terms of the insider threat is required.

3 Methods

In this section I describe the choice of methods for my study. I have conducted a qualitative study with semi structured interviews of ten Norwegian enterprises. The scientific methods used in this study applies to the theoretical framework in 'Practical Research Planning and Design' [88], in addition to given guidelines at NTNU in Gjøvik. Additionally, relevant sources and complementary frameworks have been explored.

3.1 Inductive vs Deductive Reasoning

Traditionally, research has been divided into inductive and deductive reasoning. A simplified research cycle is shown in Figure 2, based on a figure by Kowalski (1994) [80]. As shown in this figure, *inductive reasoning* starts with the *reality*, then making *observation*, before *generalizing* the observations, and ultimately forming a *theory*. While, *deductive reasoning* starts with a *theory*, makes *hypothesis*, then *observations* in order to reject or confirm hypothesis, and ultimately relate this to *reality*. I will perform the inductive part in this thesis.

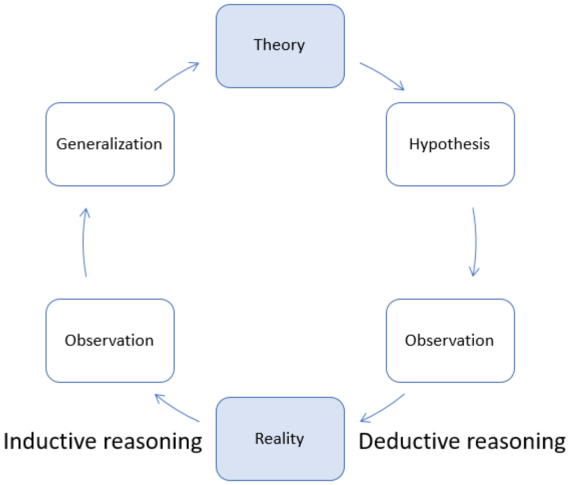

Figure 2: Inductive versus deductive reasoning

3.2 Qualitative vs Quantitative

Myers (1997) claims that quantitative research methods focus on natural science, while qualitative research methods focus on social and cultural phenomena [89]. Further, he suggest that motivations for choosing a qualitative research is the distinction between the natural world and humans; the ability to talk. Qualitative study is *not* the desired approach if the researcher is looking for "*quick results and easy answers*" [88].

A qualitative approach is suitable for description, interpretation, verification and evaluation, and will usually not identify a cause-and-effect relationship [88]. Description may "*reveal the multifaceted nature of certain situations, settings, processes, relationships, systems, or people*" [88]. While, interpretation can provide new insights, develop new concepts, or discover problems, concerning the phenomenon in focus [88]. "*The philosophical base of interpretive research is hermeneutics and phenomenology*" [89]. Hermeneutics is about interpreting textual data [90, 91, 89]. It is a combination of observation and speculation, facilitating both abductive[1] and inductive reasoning [91]. The hermeneutic circle describes the understanding of parts, and how it relates to the whole and vice versa [92, 89]. Boell and Cecez-Kecmanovic (2010) propose a new approach to literature reviews, using the hermeneutic circle. "*In this framework, the stages of searching, sorting, selecting, and acquiring as well as reading, identifying, and refining are connected*" [92].

In order to understand how Norwegian organizations approach downsizing in terms of the insider threat, I must talk to people. My study will attempt to describe and interpret the current approach, and will *not* examine cause-and-effect relationship.

Possible qualitative research designs are case study, ethnography, phenomenological study, grounded theory study, and content analysis [88]. In this study, I have applied the grounded theory.

3.2.1 Grounded Theory

Grounded theory study has its roots in sociology, and was developed by Glaser and Strauss in 1967 [88, 93]. Grounded theory is inductive [89], while first observing a phenomenon, then generalizing it, and ultimately building a theory [89, 88, 80]. However, one cannot rule out the unexplored cases [88], such as the black swans [94]. Thus, I could only develop a theory based on my findings. However, Chapter 6 Quality Assurance is a brief attempt on the deductive part, closing the research circle. This has been conducted by allowing subject matter experts and authorities within the field of security management to comment on my results and the sug-

[1] The type of reasoning whereby one seeks to explain relevant evidence by beginning with some commonly well known facts that are already accepted and then working towards an explanation. Read more: http://www.businessdictionary.com/definition/abductive-reasoning.html

gested improvements.

Literature Review

"*Qualitative researchers typically draw their data from many sources*" [88]. Nevertheless, experts disagree on how thorough the literature review should be and how data should be analyzed in grounded theory. Glaser argues, that the researcher should not gain advance knowledge early in the research process, while it may limit the possibility to be open-minded and that the theory is grounded in the data [88, 93]. Others, claim that literature review can identify gaps in knowledge and define a starting point, however avoid forming a specific hypothesis which might color the researcher's findings [88, 93].

I have performed a broad literature study while planning my work, in order to identify relevant sources and gain sufficient knowledge and understanding prior to the interviews. I did not investigate these sources in-depth prior to conducting the interviews. The intentions for this was to avoid my opinions being influenced and unintentionally affect the interview guide and the interviews. Then, while analyzing and discussing the results, I performed a deeper and improved literature review. The background chapter was completed *after* the results and discussion chapters were written. I received some of the literature sources directly from my supervisors, through courses at NTNU and former education at The Norwegian Defence University College. However, the vast majority was found through various search engines such as Oria, Google Scholar, Science Direct, ACM, Springer Link, IEEE, and Google.

Data Analysis

For data analysis, the Corbin and Strauss approach has been applied, with the four steps; (1) open coding, (2) axial coding, (3) selective coding, and (4) development of theory [88].

The results chapter aligns with open coding and axial coding, while the discussion chapter aligns with selective coding and development of theory. The data analysis started already after the first interview, by coding the transcribed interview. The first stage was *open coding*, categorizing data by connecting sections of text to specific codes within relevant topics. The second stage was *axial coding*, interconnecting categories and subcategories. The third stage was *selective coding*, creating a story line, identifying one or few core concepts. While the final stage was the *development of theory*, on how Norwegian organizations approach the insider threat while downsizing, including their suggested improvements.

Strengths and Weakness' of Grounded Theory

A grounded theory study has some disadvantages and pitfalls. As a researcher, I could have gained too much knowledge prior to the interviews, and thereby not developed a theory based on the collected and analyzed data.

Further, the interviewees might have not revealed the answers needed in order to develop a theory. Reasons for this could be that they did not consider the insider threat while downsizing a real problem, or that they did not have a plan on how to approach such problem. If so, this study would at least have discovered the current practice among the chosen sample, and could suggest improvements. This can be related to the problem of induction; the potential of the unexplored cases and the black swans [88, 94].

This kind of independent qualitative research depend a great deal on the researcher's experience, knowledge, and network. I have broad experience and knowledge, as well as a solid network providing access to subject matter experts in large Norwegian enterprises. Further, I have experience in holding a professional conversation with subject matter experts, in addition to digging deeper into specific topics.

To the authors knowledge, the Norwegian approach on the insider threat while downsizing with suggested improvements, have not been previously researched. Hence, following the grounded theory is a strength, while it provides new knowledge to this field of research.

3.3 Interviews

Given this is a qualitative study, questionnaires and structured interviews with closed questions were inadequate. Interviews in a qualitative study are either open-ended or semi-structured [88].

I sent the research topic, research problem, and research questions prior to the actual interview as part of the informed consent. The interview guide was based on the literature review, and was not shared in advance, with one exception. My approach was semi-structured, while this allowed me to ask follow-up questions and clarify possible misunderstandings. By this approach we could have a natural conversation, while I used the interview guide more as a checklist and had the flexibility to dig deeper into or skip certain topics. The interview guide was divided in two main parts, as shown in Appendix A. First some questions concerning research question one, then some questions focusing on research question two. Another exception was made, while one interview was unstructured, with post interview information sharing. I made the interviewees and their affiliated organizations anonymous, thus maintaining their right to privacy. This is echoed in Chapter 4, while some statements and claims are not cited properly. As this is individual work, I completed the interviews alone. Group interviews were avoided, with one exception. Further, voice recording simplified the interview itself, and ensured a valid transcription, without me imposing own opinions in the interviewee's statements while making notes. This allows further analysis of the transcribed interviews on a later occasion. One additional exception were made here, while one refused voice recording. A notification form concerning the use of voice recordings was submitted to, and approved by, Norwegian Centre for Research Data (NSD). We spoke Norwegian during the interviews, and the transcription was also completed in Norwegian. The intention of this approach was to capture nuances, speaking a common language, in addition to capture and understand possible tribal languages. The transcriptions were sent to the interviewees afterwards for proof reading before coding, analysis and discussion. The results of the interviews were translated to English during the coding process, and while writing the results chapter.

The translation from Norwegian to English introduces a risk of the researcher imposing own opinions while interpreting the results. This risk has been mitigated by quotation control by the quoted interviewees.

4 Results: Interviews

The interviews of ten subject matter experts employed in large Norwegian organizations provided the data and results for this study [95, 96, 97, 98, 99, 100, 101, 102, 103, 104]. The interviewees will from now on be referred to as A, B, ... J. The interviewees served within the fields of corporate security, corporate information security, corporate personnel security, and corporate information systems. Their employers are actors in various sectors such as; petroleum and energy, climate and environment, agriculture and food, defense, finance, and maritime. The size of the organizations vary from around 400 to more than 10,000 employees. Some are on the global market, but this study focus on the Norwegian market and obligations toward the Norwegian rules and regulations. Over the last decade, many enterprises in Norway have experienced downsizing. The vast majority of the enterprises in this study have recently conducted, or plan on conducting, a downsizing. However, considerations towards the insider threat in such processes have earned various attention by the participating enterprises. I carried out the interviews between January 25th and February 13th, 2017.

The interview guide, as shown in Appendix A, was structured similar to the results chapter, in chronological order. While processing the results, it became obvious that the managers have an important role, hence deserved a dedicated section in this chapter. The interview guide covered the following field of topics:

- Organizational change.
- Insider threat.
- Layoff process.
- Suggested improvements.

In terms of grounded theory, this chapter aligns with open coding and axial coding. The data analysis started already after the first interview, by coding the transcribed interview. The first stage was *open coding*, categorizing data by connecting sections of text to specific codes within the above-mentioned topics. Hence, after a coding process, the whole transcribed interview was covered by code. This process was repeated for all the interviews, and the code book was continuously improved. Coding examples were; frameworks and processes, risk analysis, and key to success, as part of organizational change. The second stage of data analysis was *axial coding*, interconnecting categories and subcategories. In this stage, I analyzed how the interviewees relate to the research questions, applying the data some context.

I developed a spreadsheet, organizing the interviews, codes, and key findings. In addition, I developed mind maps in order to group and visualize interconnections and sub categories of the findings. This was the main result of the axial coding stage.

4.1 Organizational Change

4.1.1 Frameworks and Processes

6 of 10 enterprises have frameworks for organizational change, or other policy descriptions including elements of such change process.

Most of the frameworks are derived from internal best practice, while one was similar to Hoshin Kanri and Lean [96]. Two of the interviewees reported a recent review of their change framework, with intentions of streamlining the enterprises, pushing for efficiency. Some of the interviewees are not familiar with its organizational change frameworks, and claim that the change processes are top driven HR concerns.

10 of 10 enterprises have experienced some form of organizational change in recent years. Seven have downsized or are planning on downsizing in the near future. One is merely reorganizing within current general term, while two are expanding.

4.1.2 Risk Assessment

7 of 10 enterprises performed a risk assessment as part of the change process. Such risk assessment seemed to focus on financial risk, as well as risk on the change process itself and the working environment. Two additionally included personnel security and the insider threat in their risk assessment. One enterprise performs some kind of role-based risk assessment, in order to reveal high risk positions that require special attention.

4.1.3 Key to Success

The key to success in an organizational change process seem to be; holistic planning, the perception of a fair and transparent process, openness, involvement of unions and employees, consensus, and an orderly exit process. Figure 3 shows most of the interviewee's suggestions, interpreted and grouped by me. The following paragraphs describe the interviewee's suggestions concerning the key to success in organizational change processes.

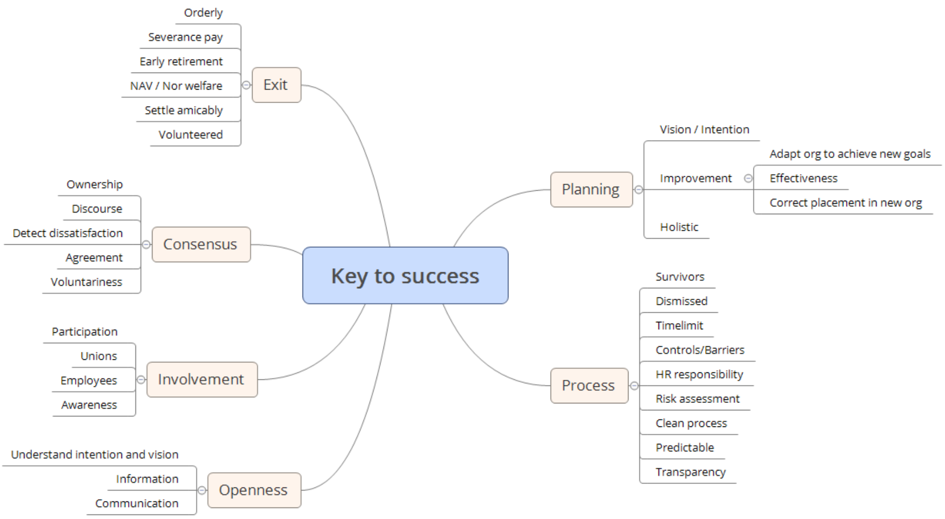

Figure 3: Key to success

Holistic planning

The enterprise should have a clear vision and intention with the change, with desired improvements. One could adapt the organization in order to achieve new goals or improve effectiveness.

Fair and transparent process

The affected employees should perceive the change as a fair, predictable, and transparent process, which does not expand in time. One must consider both the dismissed employees and the survivors, during and after a downsizing process. Establish barriers and controls in order to avoid incidents, and perform a holistic risk assessment, including the insider threat.

Openness

One of the key elements to success is open communication between the employer and the employees, with correct and definite information. The employees must understand the vision and intention for the change process.

Involvement of unions and employees

Early involvement of unions and employees are important in order to establish awareness and the sense of participation among the employees.

Consensus

Facilitate employee ownership to the process, and aim for agreement and voluntariness, even for the dismissed. During the discourse one might establish consensus, in addition to detect potential dissatisfied employees.

Orderly exit, preferably volunteered and with benefit

The exit itself must be an orderly process. Benefits such as severance pay and early retirement may increase the voluntarism for quitting. The Norwegian welfare system is strong and acts as a security net for the dismissed.

4.2 Insider Threat

4.2.1 Definitions

The interviewees were asked about how they would define insider threat. The vast majority did not seem to have developed their own formal definition. Two have adopted the CPNI definition for personnel security. The various attempts on defining insider threat included both the intentional and unintentional insider, violating security policies by e.g. sharing classified information, or damaging the organization's assets, interest, or reputation.

The results show that human resources (HR) seem to avoid the term insider threat, while it does not appreciate the employees as assets. One approach is to address this as personnel security, as defined in the CPNI-adopted security policy shared by B [96]:

> *Personnel security is a system of procedures which seek to manage the risk of staff (permanent, temporary or contract staff) exploiting, or intending to exploit, their legitimate access to an organisation's assets or premises for unauthorised purposes. (Shared responsibility between Chief HR Officer and Chief Security Officer)* [96].

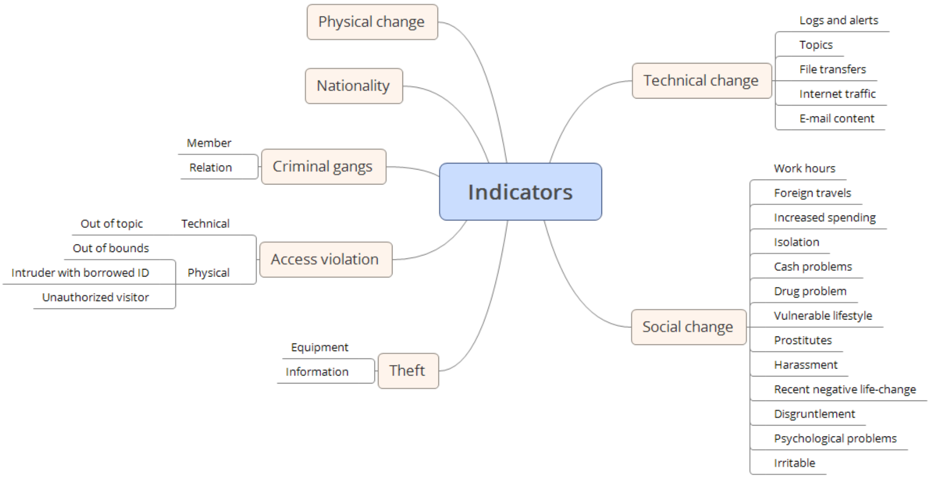

Figure 4: Indicators of insider activity

4.2.2 Indicators

The interviewees claim that the main indicator for insider activity is some kind of behavioral change. This might be both technical and social change. Figure 4 shows the suggested indicators for insider activity.

Typical technical indicators of such change might include; file access and transfers, Internet traffic, and e-mail traffic. Typical social indicators might include; abnormal working hours, increased spending, isolation, personal problems, attitude, and new travel habits. Indicators for access violation might be attempted access to a topic, area or location, which are out of scope. Other indicators could be affiliation with criminals, or theft of information or equipment.

4.2.3 Capability, Motive and Opportunity

Figure 5 shows the suggested capabilities, motives and opportunities, for malicious insider activity. The capability of an insider seems to be exploiting legitimate access to the organization's assets. The most frequently suggested motives (hence not experienced) were financial gain and revenge. While sabotage, theft, ideology, political and more, were additional suggested motives for malicious insider activity. The opportunity seemed to be downsizing processes, personal problems, in addition to insiders being forced or bribed to exploit their access.

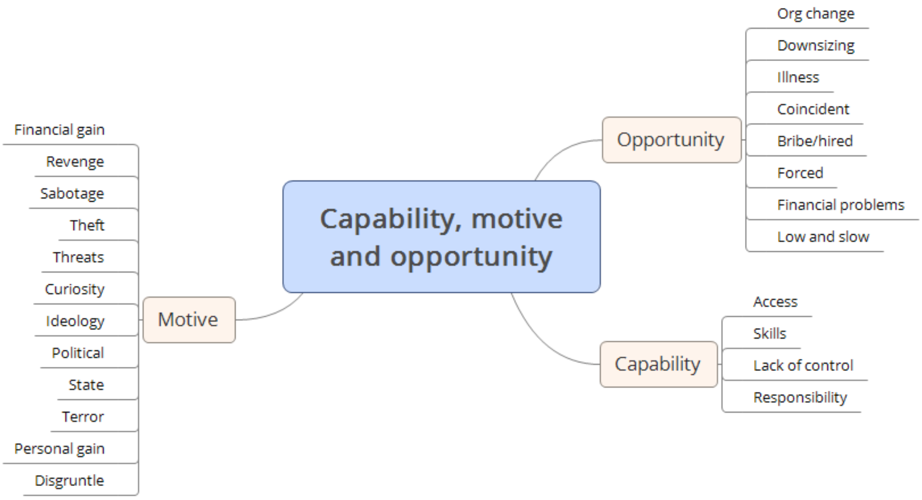

Figure 5: Capability, motive and opportunity

4.2.4 Framework or Program

5 of 10 enterprises have some kind of program or framework that consider the insider threat. However, it is a far stretch to claim all of these to be holistic insider threat programs. Figure 6 shows the suggested elements of an insider threat program.

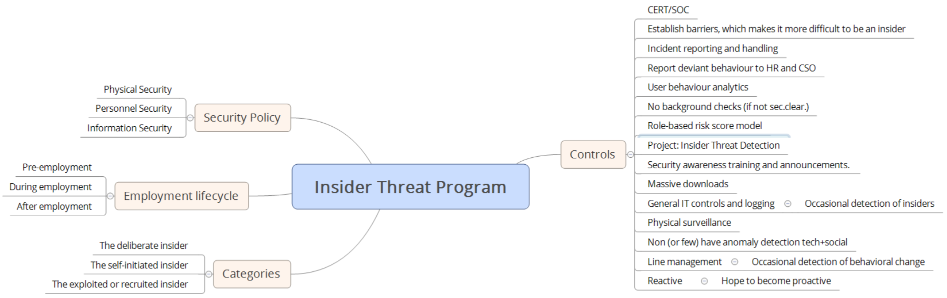
Insider Threat Program
Security Policy
Physical Security
Personnel Security
Information Security
Employment lifecycle
Pre-employment
During employment
After employment
Categories
The deliberate insider
The self-initiated insider
The exploited or recruited insider
Controls
CERT/SOC
Establish barriers, which makes it more difficult to be an insider
Incident reporting and handling
Report deviant behaviour to HR and CSO
User behaviour analytics
No background checks (if not sec.clear.)
Role-based risk score model
Project: Insider Threat Detection
Security awareness training and announcements.
Massive downloads
General IT controls and logging
Occasional detection of insiders
Physical surveillance
Non (or few) have anomaly detection tech+social
Line management
Occasional detection of behavioral change
Reactive
Hope to become proactive

Figure 6: Insider Threat Program

Most of the enterprises do not perform thorough background and identity checks. Some enterprises have a CERT (Computer Emergency Response Team) or SOC (Security Operation Center), for incident reporting and handling, in addition to standard technical controls. Some interviewees suggest establishing barriers, which makes it more difficult to launch an insider attack. Few enterprises seem to have dedicated social controls for detecting deviant behavior, leaving the manager with most of the responsibility. General technical controls and logging may lead to occasional detection of insider activity. None seem to have a holistic anomaly detection, combining the access and behavior both physically, technically, and socially. Some reported that they have security awareness training and announcements. Two interviewees mentioned that privacy concerns make it more difficult to implement sufficient controls in order to detect malicious insider activity. Some interviewees referred to CPNI, the Norwegian Security Act, and their own security policies, that divide security into the three areas; physical security, personnel security, and information security. Insider threat applies to personnel security. Mitigation of the insider threat can be conducted throughout the employment life-cycle; pre-employment, during employment, and post-employment. Two interviewees refer to CPNI and the three main types of insider behavior; the deliberate insider, the volunteer/self-initiated insider, and the exploited/recruited insider [96, 99, 53].

4.2.5 Disgruntled Employee

It is a distinction between the terms ’disgruntled employee’ and ’dissatisfied employee’. Some of the interviewees were not familiar with the term disgruntled, while some used it on a regular basis. Some interviewees claim that disgruntled is more than just being dissatisfied. You are angry on the organization or persons. You are dissatisfied with malicious intentions. Edward Snowden was by one termed as a disgruntled employee, while another claimed that a disgruntled employee was entering or had passed the point of no return. One interviewee claim that everybody has experienced being dissatisfied at work. It could be with your salary, office facilities, responsibilities and so on. However, this does not mean that you are a disgruntled employee. A dissatisfied employee is a potential risk, or has the potential of becoming disgruntled.

4.2.6 Whistleblower vs Insider Threat

Most of the enterprises seem to have a whistleblower channel, and claim the importance of it. However, it seems that there are few reported actual cases through such channel. One interviewee even claims that the whistleblower never wins, while another believes it is a difficult decision to report on good colleagues. The whistleblower channel should allow anonymous reporting, and potentially confidential dialogue, concerning critical activity [96]. Whistleblowing should primarily be reported through the manager, alternatively through the whistleblower channel [103], especially if the manager is a part of the problem [99]. The dilemma whether you are a whistleblower or a malicious insider is interesting. Snowden were again mentioned as an example in the public debate, where some claim him to be a whistleblower, while others claim him to be a malicious insider. There were split opinions among the interviewees, whether a whistleblower channel could reduce the risk malicious insider activity.

4.3 Layoff Process

4.3.1 Reasons

Reasons for dismissing an employee are various. Downsizing, misconduct, violation of security policy, or criminal act, were suggested common reasons for dismissals. Some additionally suggested health problems, unqualified employee, and the loss of security clearance as such causes. None of the interviewees reported on actual cases of criminal act in their own organization resulting in dismissals.

4.3.2 Notice

Most of the enterprises have regular notice time in accordance with Norwegian rules and regulations, typical 3 months. During the notice time, employees have both the right and obligation to relevant labor. However, this obligation may be omitted on agreement, but they still receive salaries. Situational circumstances determine whether the employee retain its access card and IT access during notice time.

4.3.3 Process and Controls

The layoff process seem to vary from much responsibility placed on the manager, to more formal processes with shared responsibilities and dedicated controls. Some of the interviewees, working with security, were not familiar with their formal layoff process. One interviewee claims this is a manager responsibility with support from HR, however not a formal process and likely no affiliated education. Some enterprises have a formal process with the notice given in a meeting-room, involving manager, HR, and security. The circumstances determine how to handle the obligation to work, IT access and physical access, administrative matters, and equipment, after the notice is given. One enterprise has both an administrative element and a security element in a layoff process [99]. The administrative part includes; revoking physical- and IT-access, closing the salary payment, and terminating all affiliations between the dismissed and the organization [99]. While the security part contains an expectation of the manager to consider which security controls that must be initiated [99]. Other controls include a reminder of a signed non-disclosure agreement, career counseling, and limit access to information and locations during notice time. Few enterprises seem to have some sort of checklist for a layoff process.

4.3.4 Severance Pay

8 of 10 enterprises offer severance pay. One does not offer severance pay, whereas one is unfamiliar with company policy on that matter. The content and size of a severance pay depends on factors such as the length of service, age, and position. A severance pay might be a few months extra salary or early retirement. Other benefits could be access to company cabin or exercise facility.

4.4 Management

Throughout the interviews it became obvious that the enterprises place much responsibility on the managers, both in terms of organizational change and personnel security. This section will provide the results concerning the topics; authorization, access management, as well as education and training.

4.4.1 Authorization

3 of 10 enterprises conduct authorization conversation with employees who have a security clearance, while 4 of 10 plan or hope on implementing a conversation or interview similar to this. H claims that the authorization conversation is about

life, while performance review is about work [102]. Organizations compliant to the Security Act must follow strict guidelines in the process of security clearance and authorization of employees, including formal education in conducting the authorization conversation. J is planning on applying an adopted authorization conversation on high-risk positions [104].

4.4.2 Access Management

All 10 interviewees stress the importance of access management both in terms of physical security and information security. Revoking the access card and IT-access will terminate access to both physical locations and digital information. However, some of the interviewees admitted that access management on dismissals have been neglected somewhat in the past.

4.4.3 Education and Training

The interviewees reported various levels of manager education and training considering personnel security and organizational change. It ranges from nothing at all, via e-learning and guidelines, to more formal education and training. None or few enterprises seem to have dedicated education on dismissals or detection of deviant behavior.

4.5 Improving Frameworks and Processes

In this section I will describe some of the suggested internal and external improvements in order to reduce the insider threat while downsizing. This will apply to research question two.

4.5.1 Internal Improvements

Some interviewees suggest starting with actually establishing frameworks or policies for organizational change, while others suggest improvements. The organizational change should be a formal process. Such framework should include a holistic risk assessment, which additionally considers the insider threat, as well as improved technical and social controls for detection and mitigation. Further, a well prepared communication plan, focusing on early and correct information aimed at both the affected employees and the entire organization. A security policy, describing physical security, personnel security, and information security, should be developed and approved by the CEO or the board. It is additionally suggested to use the term 'personnel security' instead of 'insider threat', while personnel security is softer and appreciate the employees as assets as opposed to threats.

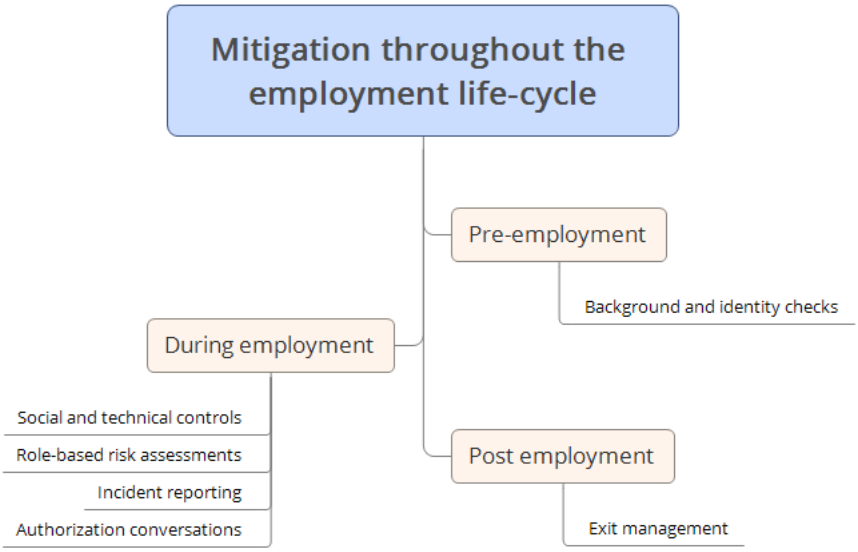
Mitigation throughout the employment life-cycle
Pre-employment
Background and identity checks
During employment
Social and technical controls
Role-based risk assessments
Incident reporting
Authorization conversations
Post employment
Exit management

Figure 7: Mitigation throughout the employment life-cycle

Some interviewees have suggested mitigation throughout the employment life-cycle as shown in Figure 7; pre-employment, during employment, and post-employment [96, 99]. This includes background and identity checks, authorization conversations, controls, role-based risk assessment, incident reporting, and exit management. A framework should describe responsibilities concerning downsizing and personnel security, shared between security officer, HR, and managers.

4.5.2 External Improvements

Various publicly available guidelines and templates, as well as affiliated education, were proposed by some interviewees. This might include general topics such as:

- How to approach the insider threat while downsizing.
- Authorization conversation adjusted for private sector.
- Management ethics guidelines.

Some enterprises would additionally prefer wider authority and guidelines on how to perform pre-employment background and identity checks.

4.6 Summary Results

This section is a summary of the results aligned with the research questions.

Research question 1

How do Norwegian organizations approach a downsizing in terms of the insider threat?

Few of the enterprises seem to have a holistic approach toward the problem:

- 6 of 10 have framework for organizational change.
- 10 of 10 have been through or plan an organizational change.
    - 7 of 10 have downsized or plan on downsizing.
    - 1 of 10 is only reorganizing.
    - 2 of 10 are expanding.
- 7 of 10 did risk assessment (some included insider threat).
- 5 of 10 have some kind of insider threat program.
- 3 of 10 have some kind of authorization conversation.
    - 4 of 10 plan or hope to implement.
- 8 of 10 offer severance pay.
- 10 of 10 consider access management important.
- Most consider the insider threat a serious problem.

Research question 2

How can the insider threat on dismissals be reduced through improved downsizing processes?

Some of the enterprises do not have organizational change frameworks. They acknowledge that development and implementation of such is a good start. Then, while downsizing, they should conduct a holistic risk assessment, including the insider threat. It is also suggested to establish technical and social controls throughout the employment life-cycle; pre-employment, during employment, and post-employment. Such controls might include structured identity and background checks, social and technical behavioral change detection, holistic access management, and transform from a reactive towards a proactive approach. Some additionally endorse the value of some kind of authorization conversation, and plan on implementing such in their organization.

Suggested external improvements include various publicly available guidelines, templates, and education, in addition to wider authority to perform pre-employment background and identity checks.

5 Discussion

The literature review and the interviews have provided me with knowledge and findings on how Norwegian organizations approach the insider threat while downsizing. Additionally, the interviewees have suggested internal and external improvements on the matter. In terms of grounded theory, this chapter aligns with selective coding, identifying one or few core concepts, and the final phase of developing a theory on how Norwegian organizations manage the insider threat in downsizing processes. Thus, answering research question 1.

It is fair to claim that Norway is a safe place to live and work. The Norwegian Working Environment Act ensures rights and obligations for both the employer and the employee. Then we have NAV's services, benefits and pensions, in case of e.g. unemployment, sickness, or birth of a child. This provides the employees with strong rights and a solid safety net. It might have an influence on how Norwegian companies approach a downsizing process, and how a dismissed employee reacts to it. Hence, performing a downsizing in Norway might be more difficult than in the rest of Europe and the US.

My analysis has identified management as a key element in order to mitigate the insider threat while downsizing. Starting with top management in the planning phase, then transferring more responsibility on the middle management in the execution phase.

By selective coding, I will use the Plan-Do-Check-Act (PDCA) cycle [105], in order to create a time-line that connects the key findings of the results. This is additionally the structure of this chapter, as shown in Figure 8. The first three steps will focus on research question 1, while the latter step will focus on research question 2. The intention of this structure is to guide the reader through a change process, while discussing the findings. Further, this will show how other categories and concepts relate to management, as the core of this grounded theory. In the *plan* section, I will discuss frameworks, policies and plans. In the *do* section, I will address security culture, actions, mitigation and controls. Then, I will suggest how the participating enterprises approach the problem, according to a maturity model, in the *check* section. I will discuss the suggested improvements in the *act* section.

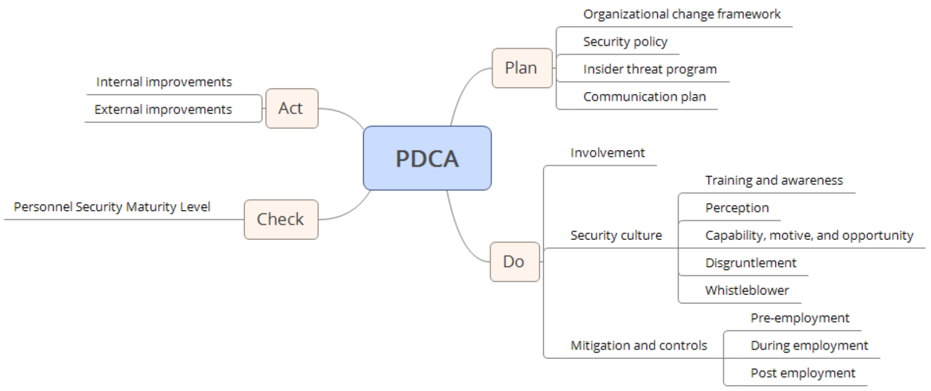

Figure 8: PDCA cycle

5.1 Plan

5.1.1 Organizational Change Framework

The results show that all participants have experienced some form of organizational change in recent years. Not all seem to have developed and follow a certain framework or process for such change. My study will not discuss strengths and weaknesses of various change processes. Nevertheless, an organizational change should be planned and follow a known procedure. Organizational change frameworks are described in Chapter 2.

The top management could facilitate a predictable process and early involvement of unions and employees, by determining the roles and responsibilities in change process. This is echoed during the interviews and in Norwegian research [34, 7].

The Norwegian Working Environment Act states that a risk assessment is mandatory in order to reduce the uncertainty among the employees [21]. The results show that 7 of 10 enterprises performed a risk assessment as part of the organizational change, whereof only two included the insider threat. This included role-based risk assessment, identifying high risk positions and affiliated controls for mitigating the risk, and access control on affected employees while downsizing. Organizations could reduce uncertainty by conducting a continuous and holistic risk assessment which includes personnel security, in addition to a specific risk assessment during an organizational change. According to the crime and security survey in Norway in 2015 (KRISNO 2015), 23% of the participating organizations conducted a written risk assessment [12].

5.1.2 Security Policy

Security is often divided into the three areas; physical security, personnel security, and information security. A security policy could contain e.g. statement of purpose, definitions, as well as security roles and responsibilities [35].

The managers hold a large share of the security responsibility on a daily basis, and certainly during a downsizing process. The general obligations can be defined in a security policy, while specific obligations can be specified in e.g. a change framework.

Some interviewees prefer the term personnel security rather than insider threat, while it is softer and appreciate the employees as assets as opposed to threats. CPNI seems to share this approach in their guidelines for personnel security [52].

5.1.3 Insider Threat Program

The results show that 5 of 10 enterprises have some kind of insider threat program. However, it is a far stretch to claim all of these to be holistic insider threat programs.

Some interviewees referred to CPNI templates and the Norwegian Security Act, dividing security into the three areas; physical security, personnel security, and information security. Chabinsky (2014) claims that the security departments and HR must cooperate in order to achieve a successful insider threat program [75]. Thus, it would be wise to aim for a holistic approach for the risk and security management in order to mitigate the insider threat. This is not a one-man job inside his own silo. The responsibilities might be shared between e.g. security officers and human resources on the corporate level, as well as with managers at all levels in the hierarchy. At the end of the day, the managers play an important role in mitigating and detecting insider activity, in terms of behavior and motivation. In addition to the social controls, one must pay attention to the technical and physical controls. More on this later.

Some interviewees referred to the three main types of insider behavior; the deliberate insider, the volunteer/self-initiated insider, and the exploited/recruited insider [96, 99]. My study focuses on the self-initiated insider during or after a downsizing process. However, a holistic insider threat program should consider all types of insider behavior.

5.1.4 Communication Plan

The results show that the perception of a fair and open process is important. A well planned and executed communication plan could facilitate this. This is supported by sources in Chapter 2 [7, 34]. It is the top management who determines the communication strategy, while the line managers play an important role in the actual communication with the employees. The employees should understand the intention and vision of the change process. The interviewees had various perceptions concerning how early in the downsizing process information should be announced to the employees. One approach is to release information early in order to reduce uncertainty and gossip. However, premature information with potential to affect the stock price, could increase the risk of insider trading. In addition to timing, the information released should be correct, and aimed at both the dismissed and the survivors of a downsizing. This is supported by literature in Chapter 2 [36, 41].

5.2 Do

5.2.1 Involvement

Rørvik (2010) claims that the union could provide the management with employee's experiences and reactions to the downsizing measures [7]. My results support this by interviewees claiming that, early involvement of unions and employees are important in order to establish awareness and the sense of participation among the employees. If the organization is aiming for consensus during a downsizing process, early involvement of and transparency towards unions and employees seem reasonable. Early involvement could also reduce rumors in the initial stages of the downsizing.

5.2.2 Security Culture

Organizational culture can be created and influenced by proper selection, training, and socializing of the employees [29]. It is a managerial responsibility to create a healthy security culture, encouraging the desired behavior and reporting critical incidents and deviant behavior. A healthy security culture could reduce the risk of employees transforming into malicious insiders. This is supported by the social learning theory [17, 63]. Additionally, a malicious insider might influence ignorant colleagues by social engineering.

Training and Awareness

As emphasized above, the managers at all levels play very important roles in a downsizing process. In order to fully prepare the managers for this challenge, they need a set of skills, a toolbox, and sufficient support and resources. The interviewees reported various levels of manager education and training considering personnel security and organizational change. It ranges from nothing at all, via e-learning and guidelines, to more formal education and training.

According to Mishra and Dhillon (2006), security training increases the awareness, prevents breaches due to ignorance, and prevents security attacks proactively [63]. However, in a recent study CLTRe claims that they only noticed a weak correlation between formal training, knowledge, and behavior, and suggest additional implementation of a holistic, risk-based approach [106].

As a foundation, the managers should have formal managerial and organizational education, and earn the position due to management skills, not seniority. The most experienced technician is not necessarily the best suited manager. Further, managers should have formal education and training in security management in general and personnel security in particular. More specific, such education might include administrative matters, general security, information security, personnel security and authorization conversation. It is likely the managers who are best suited for detecting deviant behavior. The theory of anomie could help us to understand deviant behavior [63].

Perception

As described in Chapter 2; it is the perception of how the downsizing process was conducted that matters, concerning employee motivation [36, 37]. This is supported by H who claims that a happy exit yields good behavior afterwards [102]. Hence, both the intended and the unintended effects on the employees' perception should be assessed while downsizing. Once again, the perception of both the dismissed and the survivors of the downsizing should be considered.

Capability, Motive, and Opportunity

Capability is achieved by being on the inside of the security perimeter, both physically and logically, in addition to having insider knowledge. These factors, and others, give the insider the capability of causing harm on the employer's assets.

The results show that suggested primary motivation were financial gain and revenge. While sabotage, theft, ideology, and political were additional suggested motives for insider activity. Nevertheless, none of the interviewees shared knowledge of insider activity in their Norwegian departments. Hence, the suggested motivations were not self-experienced, rather qualified assumptions. A CPNI study support the suggestion of financial gain being the primary motivation, but claims that revenge is further down the list [53].

In terms of my study, the opportunity arises while downsizing. An employee might have had both the capability and motive for becoming an insider for a while, and is triggered by the downsizing process.

Disgruntlement

As shown in Chapter 4, interviewees suggest that it is a distinction between the terms 'disgruntled employee' and 'dissatisfied employee'. Disgruntled is more than just being dissatisfied. You are angry on the organization or persons. You are dissatisfied with malicious intentions. Further, a dissatisfied employee is a potential risk, or has the potential of becoming disgruntled. This is somewhat supported by Greitzer et al. (2012) who have defined disgruntlement [9]. Both an international study [14] and NSM [45] claim that the insider showed signs prior to the incident, of being or becoming a malicious insider or being perceived as disgruntled.

The managers have an opportunity to both mitigate the transaction from dissatisfied towards disgruntled, in addition to detecting the behavioral change. Thus, once again the manager play an important role concerning the insider threat while downsizing. However, the managers must be educated and trained in order to be capable of this.

Whistleblower

The Working Environment Act supports whistleblowing [20], while the Security Act support protection of classified information [44] . Additionally, organizations not compliant to the Security Act, sometimes require the employees to sign a non-disclosure agreement. The results show that most of the enterprises seem to have a whistleblower (WB) channel, and claim the importance of it. However, it seems that there are few reported actual cases through such channel. The primary routine for whistleblowing seems to be through the line manager, and secondary through the anonymous WB channel. The weakness of this routine is that once you have reported to the line manager, your anonymity is blown before reporting through the WB channel. Thus, if the manager refuses to act on the notification, the notifier's loyalty and trust towards the manager is tested. Snowden is an example in the public debate, where some claim him to be a whistleblower, while others claim him to be a malicious insider.

5.2.3 Mitigation and Controls

The results suggests mitigation of the insider threat throughout the employment life-cycle, as shown in Figure 7 on page 36. Additionally, it seems smart to focus on mitigation throughout the downsizing process in particular. In this chapter, this is described by the four stages; plan, do, check, and act. I am currently discussing the *do* stage.

Pre-employment

The mitigation of a potential insider threat starts prior to employment. Background and identity checks could reduce the risk of employing potential future malicious insiders. The interviewees acknowledge that such controls are important, however not all seem to have given it sufficient attention. This is supported in KRISNO (2015) [12]. NSR has issued guidelines on how to perform a background check [83], and the diploma registry have become operative [84]. Enterprises that have shortcomings concerning pre-employment screening, could benefit from applying such measures. It is also possible to hire professional headhunters in this process.

Those compliant to the Security Act have extended possibilities in conducting a thorough pre-employment screening. This includes considering criminal records, credit rating, drug or alcohol abuse, and affiliation with criminal organizations.

During employment

As shown in the results, the main indicator for insider activity is some kind of technical or social behavioral change. This includes; file access and transfers, Internet traffic, e-mail traffic, abnormal working hours, increased spending, isolation, personal problems, attitude, and new travel habits. Figure 4 on page 30 shows the suggested indicators for insider activity. These results are mostly supported by Greitzer et al. (2012), suggesting 12 psychosocial risk indicators [9]. In this matter, it is fair to promote the recently suggested ontology for insider threat indicators by Costa et al. [76]. Such ontology could ensure that we use common expressions and procedures, in mitigating the insider threat.

The results show that none of the participating enterprises seem to have a holistic anomaly detection procedure, combining the access and behavior both physically, technically, and socially. Harkins (2016) seem to support this, as described in Chapter 2 [78]. However, this is a difficult topic, while the right to privacy must be considered as well. Two interviewees mentioned that privacy concerns make it more difficult to implement sufficient controls in order to detect malicious insider activity. Enterprises must adhere to both the national and international rules and regulations, such as the Working Environment Act [20], the human rights, and the upcoming EU General Data Protection Regulation (GDPR) [57]. The Personal Data Act has been active in Norway since April 2000. Norwegian enterprises will likely have to implement certain changes in terms of privacy. However, the implementation of GDPR will continue the key principles of the Personal Data Act, as well as contribute to a more harmonized regulatory framework in Europe [58]. This might result in a harmonized approach for Norwegian and European Enterprises in terms of insider threat detection as well.

Whitman and Mattord (2011) suggest a set of 20 access controls [35]. The set includes access control policy and procedures, account management, separation of duties, least privilege, and remote access [35]. The results show that all enterprises consider access control important, especially while downsizing. However, the results revealed that not all enterprises have a formal policy and procedure on this matter.

In my results, 3 of 10 enterprises have authorization conversations, while 4 are planning or hope to implement a conversation or interview similar to this. One interviewee reported performing role-based risk assessment that suggests if special attention is required [104]. This seems similar to the a psychosocial model developed by Greitzer et al. (2012), which *assess an employee's behavior associated with an increased risk of insider abuse* [9]. NSM has developed a manual on authorization and authorization conversation, aimed at those compliant to the Security Act [85]. This manual is not suited for enterprises that are not compliant to the Security Act.

However, elements of this manual might be useful in order to assess if an employee should be granted a certain authorization, and thereby access to business confidential information. One interviewee suggested that Finance Norway could develop a manual on how to conduct an authorization conversation in the finance sector.

One interviewee claims that barriers may reduce the risk of insider activity [97]. In this case, barriers might include intrusion detection and prevention system. This is supported by crime theories such as the situational crime prevention theory [17, 18], rational choice theory [17], and the general deterrence theory [65]. These theories suggest a decision for committing criminal act is the result of a cost benefit assessment. Hence, a incident could be avoided if the malicious insider have a weak motive and the risk of being discovered is high. Again, barriers must adhere to rules and regulations in terms of privacy.

Post-employment

Whitman and Mattord (2011) suggest different aspects while downsizing, including access control, hostile and friendly departure, and exit interview [35]. This, in addition to other measures, can be termed 'exit management'. In contrast to this, the Norwegian Working Environment Act states the termination of employment relationships, including periods of notice and multiple variants of protection against dismissal [20]. The results show that few of the enterprises seem to have some sort of checklist on exit management. As described in Chapter 2, Whitman and Mattord (2011) suggest performing some tasks when an employee prepares to leave the organization [35]. They consider a downsizing as a hostile departure, and suggest revoking access before the employee has a chance to exploit it. Revoking access early might reduce the risk of an insider attack. However, this will likely add fuel to potential motivation for launching a post-employment attack. This could be a prepared attack, such as a logical bomb to delete or compromise information, or exploiting knowledge in order to damage the reputation or relations.

The results show that Norwegian organizations seem to follow a softer approach while downsizing, as opposed to the recommendations from Whitman and Mattord (2011). Most of the organizations have regular notice time in accordance with Norwegian rules and regulations, typical 3 months. During the notice time, employees have both the right and obligation to relevant labor. However, this obligation may be omitted on agreement, but they still receive salaries. Situational circumstances determine whether the employee retain its access card and IT access during notice time. Additionally, few of the enterprises in my study seem to perform an exit interview, which could include a reminder of a non-disclosure agreement.

Some interviewees referred to NAV's services and benefits in case of unemployment. This provides the employees with strong rights and a solid safety net. It might have an influence on how Norwegian companies approach a downsizing process, and how a dismissed employee reacts to it.

My results show that 8 of 10 enterprises have severance pay. This could likely reduce risk of the insider threat while downsizing. However, as one interviewee claimed; *when a company is bleeding cash, it is not feasible to offer more than what is required by law* [96]. In this case, it is even more important with management attention and technical controls during and after the downsizing.

Norwegian studies claim that downsizing increase the risk of psychosocial consequences for the dismissed [40]. Such psychosocial consequences while downsizing might increase the risk of an insider attack. Some of the participants in my study offer employees career counseling and other support while downsizing, in order to aid the job seeking process and psychosocial challenges. This again, could reduce the risk of an insider attack.

My results show that one must consider both the dismissed employees and the survivors, during and after a downsizing process. Thus, measures while downsizing should not only be aimed at the dismissed. A survivor might turn rough, if loosing good colleagues or perceives the downsizing as a negative process. Perhaps he/she did not earn the desired position after a change process. Thus, the survivors might deserve special attention as well.

5.3 Check

5.3.1 Personnel Security Maturity Level

In order to assess the maturity level of my sample, I have developed a simple Personnel Security Maturity Model (PSMM) as shown in Figure 9. My model is based on my results, CPNI's PSMM [66], NSM's maturity level for security management [67], and CMMI Institute's Capability Maturity Model Integration (CMMI) [68]. These models are briefly described in Chapter 2.

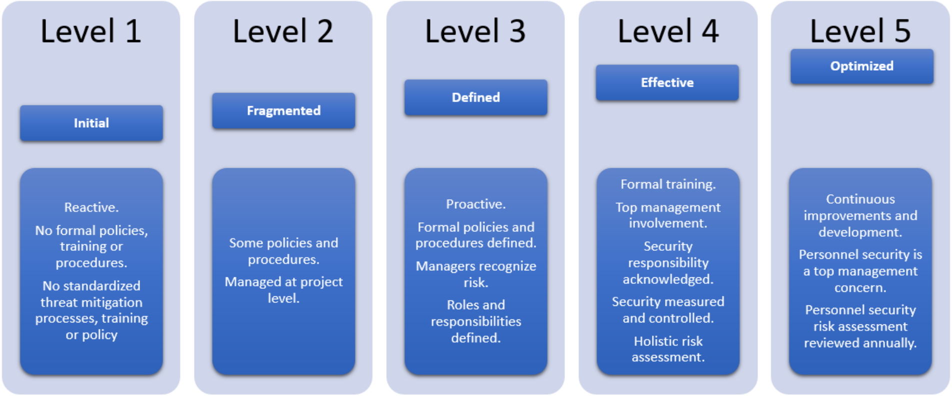
Level 1
Initial
Reactive.
No formal policies, training or procedures.
No standardized threat mitigation processes, training or policy
Level 2
Fragmented
Some policies and procedures.
Managed at project level.
Level 3
Defined
Proactive.
Formal policies and procedures defined.
Managers recognize risk.
Roles and responsibilities defined.
Level 4
Effective
Formal training.
Top management involvement.
Security responsibility acknowledged.
Security measured and controlled.
Holistic risk assessment.
Level 5
Optimized
Continuous improvements and development.
Personnel security is a top management concern.
Personnel security risk assessment reviewed annually.

Figure 9: Personnel Security Maturity Model

Based on the results and interpretation of the data, I assess the participating enterprises on average reaching level 3. Some of the organizations seem to have a reactive approach towards the insider threat, while others are more mature applying a proactive approach. This includes policy, procedures and training, holistic risk management, management attention, as well as technical and social controls for threat mitigation. I assessed my sample not reaching level 4, while they do not seem to have relevant formal training and a holistic risk assessment that includes personnel security. The results indicate that on average, the insider threat does not earn special attention while downsizing. Additionally, few of the enterprises seem to measure the level of security, and implement sufficient technical and social controls. This qualitative claim is supported by my results, concerning the share of enterprises who reported having; organizational change framework, risk assessment, insider threat program, authorization conversation, access management, as well as education and training. These results are shown in Figure 10, with the average score of 58%. Transferred to the PSMM as shown in Figure 9, this aligns with level 3.

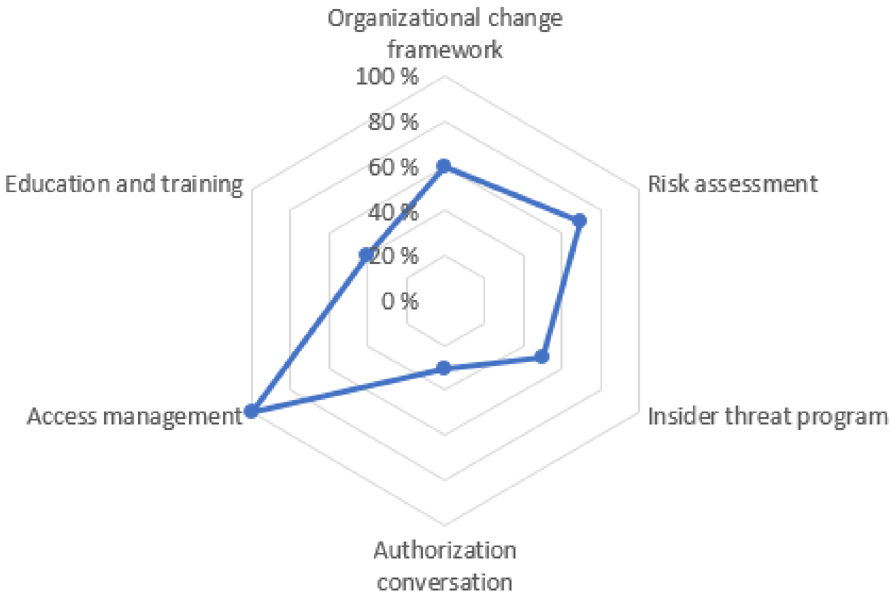

Figure 10: Personnel Security Maturity Level

5.4 Act

This section will discuss the improvements suggested by the interviewees, and partially compared with international best practice.

5.4.1 Internal Improvements

Some interviewees suggest starting with actually establishing policies, procedures and training, concerning organizational change and personnel security. Further, enterprises should implement a holistic risk assessment which includes the personnel security assessment. Carnegie Mellon University (2012) suggests 19 best practices in mitigating the insider Threats [50], while Whitman and Mattord (2011) suggest eight personnel security controls [35]. These two approaches are briefly described in Chapter 2, and are mostly echoed in my results and further discussed in this chapter.

The results indicate that the general ability to detect and respond to insider activity is low. Regular technical controls might detect such activity by chance, while continuous management attention and measures such as authorization conversations might detect deviant social behavior. None of the participants of my study seem to combine sufficient technical and social controls, in order to detect an undesired behavioral change. On the other hand, employees have the right to privacy. The results show the suggested mitigation by both technical and social controls throughout the employment life-cycle. This focus on both social and technical controls are supported by Saathoff et al. (2013) [19] and Kowalski (1994) [80].

5.4.2 External Improvements

The results show that some interviewees would appreciate various publicly available guidelines and templates, as well as affiliated education. In addition to this, some would like wider authority and guidelines on how to perform pre-employment background and identity checks.

As described in Section 2.1.2, KMD have issued a personnel policy by readjustment procedure in the government sector [25]. Despite it is aimed at the government sector, it holds many topics relevant for the private sector as well. This guideline does not consider the insider threat while downsizing. However, the suggested actions and controls might have an indirect effect, thus mitigating this threat.

NSM has issued guidelines for authorization and how to perform an authorization conversation, aimed at those compliant to the Security Act [85]. One interviewee desires such guidelines aimed at specific sectors as well, issued by e.g. the Norwegian Communications Authority (NKOM), Finance Norway, or the Norwegian Water Resources and Energy Directorate (NVE).

NSR issued guidelines on how to perform background checks some years ago [83]. This is available for purchase on the NSR web page. In addition to this, you might hire headhunter firms, specialized in both recruiting the right candidate, as well as performing a thorough background and identity check. The consequences of hiring the wrong candidate may firstly cost a lot of money, and ultimately result in bankruptcy [107]. NSR, KRIPOS, PST and NSM are working on guidelines for what happens in the period before, during, and after a working relationship [107].

5.5 Summary of Discussion

I have now completed the chain of inductive reasoning, which is the left side of the research circle in Figure 2 on page 21. This section contains a short summary concerning the two research questions.

Research Question 1

How do Norwegian organizations approach a downsizing in terms of the insider threat?

This question has been answered in the *plan*, *do*, and *check* sections in this chapter. The short answer to the research question is that the enterprises in my study overall are on maturity level 3, on a scale from 1 to 5. The key findings, and the core theory of this study is that the managers play very important roles both in general, and while downsizing and mitigating the insider threat. The ability to detect and respond to insider activity seem to be low, and malicious insider activity might be detected by chance.

Research Question 2

How can the insider threat on dismissals be reduced through improved downsizing processes?

This question has been answered in the *act* section of this chapter. Some enterprises should start by implementing formal policies, procedures, and training, in terms of organizational change, risk management, and personnel security. Then the managers should be educated and trained, in order to improve the security culture. Mitigating the insider threat should earn attention throughout the employment life-cycle, by a combination of social and technical controls. However, with adherence to rules and regulations, such as the GDPR.

5.6 Critique

This section contains some thoughts on possible limitations and weaknesses with the chosen research method.

It could have been a limitation to the study while only conducting ten interviews. However, during the interviews the key findings was repeated in various forms, and it is not likely that more interviews would change this significantly.

Further, I only interviewed large enterprises, whereas the vast majority of Norwegian companies are SMEs. One can assume that a small company with 5-10 employees should focus on innovations and deliveries, not policies and procedures. Additionally, separation of duties and least privileges are likely not the way a SME operates. SMEs might additionally not consider the insider threat as a problem worth the attention. Hence, interviewing SMEs in this study would likely affect the findings significantly. By excluding SMEs, I could form a theory on the Norwegian downsizing approach for large enterprises.

The researcher's experience and ability to gain access to relevant interviewees might be a weakness or strength. The interviewees could have been friends or colleagues in similar positions, enterprises, and sectors. However, the result show variance in terms of both position in enterprise, size of enterprise, and sector.

The interviews was conducted in Norwegian, and later interpreted and transcribed while analyzing the results. While this study aims at developing a theory concerning the Norwegian approach, it could benefit from being completed in Norwegian. However, given most of the literature is in English, this was also the preferred language while writing this thesis.

6 Quality Assurance

In terms of the research circle as shown in Figure 2 on page 21, my grounded theory is a result of the inductive reasoning part. This chapter will be a brief attempt on the deductive part, closing the research circle. This has been conducted by allowing subject matter experts and authorities within the field of security management to comment on my results and the suggested improvements.

6.1 NSM

"*The Norwegian National Security Authority (NSM) is a cross-sectoral professional and supervisory authority within the protective security services in Norway*" [54]. Following are the comments from the head of personnel security at NSM, shared by e-mail correspondence during May 2017 [108].

> *NSM is obviously concerned with the insider threat issue. This is especially important to us when someone needs access to classified information and requires a security clearance. In accordance with Section 21 of the Security Act, in the process of whether a person can obtain a security clearance, his/her reliability, loyalty and sound judgment are assessed. The insider threat issue has a natural place in this assessment. We are continuously working on improving our own guidance to both security clearance authorities and enterprises in this regard. This primarily affects enterprises that are compliant to the Security Act. However, we see that the same challenges / vulnerabilities are also applicable to unclassified information, and we therefore focus on reusing some of our expertise in this regard. NSM has, together with NSR, Kripos, and PST, been an active contributor to the work of creating a common guideline for background checks of employees. NSM clearly sees the need for enterprises to work more systematically with these challenges. NSM will continue to focus on the insider threat issue in the future in various ways.*

Further, NSM emphasizes that their authorization conversation focus on organizations compliant to the Security Act, and is not directly transferable to areas outside this Act.

NSM does not question my findings, and endorse that this topic is being illuminated.

6.2 NorSIS

"*The Norwegian Center for Information Security (NorSIS) is an independent organization and partner to the government, businesses and research facilities in the subject of cyber security*" [109]. Following are NorSIS' statements concerning my results, shared during an interview at Gjøvik 20th April 2017 [110].

NorSIS mostly focus on SME, not large enterprises, and is therefore unable to comment on whether the results are representative for large Norwegian enterprises.

NorSIS claims that both the term 'insider threat' and actions for mitigation this threat are somewhat tabooed in Norwegian organizations. SMEs in Norway do not seem to focus enough on security management system. Hence, their first priority should be to establish such system before eventually implementing an insider threat program. In SMEs one have to trust each other. Often every employee has access to all of the information in the company, and this might be the best way of doing business. However, it is a sliding transformation from SME to large enterprise, and at some point, the enterprise should consider segregation of access to certain information. For SMEs, business partners might grant more and more trust and access over time, thus increasing the potential for insider threat considerations. NorSIS has experienced that SMEs conduct background checks of partners and suppliers, but neglect a similar pre-employment screening.

NorSIS does not develop or share guidelines on the insider threat while downsizing, authorization conversation for private sector, or management ethics.

6.3 NSR

"*The Norwegian Business and Industry Security Council (NSR) is a member organization that serves the Norwegian business sector in an advisory capacity on matters relating to crime*" [111]. Following are NSR's statements concerning my results, shared by e-mail correspondence during April-May 2017 [112].

NSR has for many years, through their Crime and Security Survey in Norway (KRISNO), asked questions about the extent to which Norwegian enterprises actually do perform written risk assessment, background and identity check, as well as reference check and diploma verification. The findings in KRISNO 2015 and the findings in this thesis seem to point towards similar conclusions.

NSR have issued guidelines on how to perform a background check of employees. Additionally, NSR, KRIPOS, PST and NSM are working on guidelines for actions in the period before, during, and after a working relationship. These guidelines will address several of the concerns emphasized in this thesis, and will hopefully be released before the summer this year (2017). In addition to this, NSR proposed in 2010 the creation of a witness portal in order to prevent counterfeiting and facilitate the verification of diplomas. This has now seen the light of day.

6.4 Summary Quality Assurance

NSM, NorSIS and NSR represent a large set of data and observations through their audits, surveys and close interaction with both SMEs and large enterprises, both compliant and not compliant to the Security Act. Thus, act as the observation on the deductive side of the research circle as shown in Figure 2 on page 21. None of the subject matter experts, with their background and expertise, question my findings.

NSM is obviously concerned with the insider threat issue, especially in terms of the Security Act. However, NSM endorses the reuse of their expertise for enterprises that are not compliant to the Security Act. NSM has, together with NSR, Kripos, and PST, been an active contributor to the work of creating a common guideline for background checks of employees. NSM clearly sees the need for enterprises to work more systematically with these challenges.

NorSIS focus on SMEs. Nevertheless, NorSIS is considered an authority concerning information security. NorSIS claims that SMEs in general cannot implement a strict insider threat program, while often every employee has access to all of the information in the company. However, some elements of such program might be relevant for SMEs as well.

NSR reveals that NSR, KRIPOS, PST and NSM are working on guidelines for actions in the period before, during, and after a working relationship. This will hopefully be released before the summer this year (2017). The findings in KRISNO 2015 and the findings in my study seem to point towards similar conclusions.

7 Conclusion

Many Norwegian enterprises in various sectors have been downsizing over the last decade. Among the current threats to organizations, the insider threat could be the most significant. This threat might be increased during or after a downsizing process.

This research examined how the Norwegian organizations approach a downsizing in terms of the insider threat. Additionally, the interviewees have suggested improvements in such process. Ten subject matter experts in large Norwegian enterprises were interviewed. These subject matter experts serve in various industry sectors such as; petroleum and energy, climate and environment, agriculture and food, defense, finance, and maritime. The size of the organizations varies from around 400 to more than 10,000 employees. The results of these interviews have been discussed and partially compared with international practice. Then, authorities within the field of Norwegian security management have commented on the findings and the suggested improvements. This is a qualitative study that describes and interprets the Norwegian approach, which provides strong rights for the employees, and does not examine cause and effect relationships.

The first research question focus on how Norwegian organizations approach a downsizing in terms of the insider threat. This question has been answered in the *plan*, *do*, and *check* sections in Chapter 5. The results indicate that the participating enterprises on average reach level 3 on a scale 1 to 5, in accordance with the Personnel Security Maturity Model (PSMM). In this model, level 3 suggest that an enterprise applies a proactive approach, has formally defined policies, procedures, roles and responsibilities, and that managers recognize risk. The general ability to detect and respond to insider activity seem to be low, and malicious insider activity might be detected by chance. In addition to this, the results indicates that on average, the insider threat does not earn special attention while downsizing.

The key findings, and the core theory of this study is that the managers play important roles in mitigating the insider threat while downsizing. It is the managers who knows the employees, and make decisions concerning security management, and are key players in building a healthy security culture. Continuous management attention and measures similar to the authorization conversations developed by NSM, might aid in detecting deviant social behavior. Given this important role, it is surprisingly low level of education and training aimed at personnel security management and line management.

In terms of formal policies and procedures, the results indicate that some enterprises are somewhat immature with a reactive approach. However, other enterprises apply a more proactive approach with holistic policies and procedures, formally defined and trained. None of the participants of this study seem to combine sufficient technical and social controls, in order to detect an undesired behavioral change. Nevertheless, the enterprises must adhere to both national and international rules and regulations.

The second research question focus on improvements in downsizing processes. This question has been answered in the *act* section of Chapter 5. As a foundation, enterprises should have established formal policies, procedures, and training, in terms of organizational change, enterprise risk management, and personnel security. As emphasized above, the managers at all levels play important roles in a downsizing process. In order to fully prepare the managers for this challenge, they need a set of skills, a toolbox, and sufficient support and resources. The managers should be educated and trained, in order to improve the security culture and detect deviant behavior. Further, some enterprises could transform their approach from reactive towards proactive. Mitigating the insider threat should earn attention throughout the employment life-cycle, by a combination of social and technical controls. However, with adherence to rules and regulations, such as the GDPR in terms of privacy.

Suggested 'external' improvements include various publicly available guidelines and templates, as well as affiliated education. In addition to this, some would like wider authority and guidelines on how to perform pre-employment background and identity checks. The new common guideline for background checks of employees, developed by NSR, KRIPOS, PST and NSM, seems to answer parts of the suggested improvements.

NSM, NorSIS and NSR represent a large set of data and observations through their audits, surveys and close interaction with SMEs and large enterprises, both compliant and not compliant to the Security Act. They have provided comments on the findings and the suggested improvements. This study has applied inductive reasoning, whereas their comments act as the observation on the deductive side of the research circle. None of the subject matter experts, with their background and expertise, question the findings.

To the authors knowledge, there have not been similar previous research, on how Norwegian organizations approach a downsizing in terms of the insider threat.

8 Further Work

This study has focused on the inductive reasoning part of the research circle, with a brief deductive approach in the quality assurance chapter. A natural step in closing this research circle, is to conduct a study applying deductive reasoning. Thus, I would suggest further work and research as follows:

- Quantitative research with questionnaires to Norwegian organizations, measuring the personnel security maturity level while downsizing. This could be a complete deductive part of the research circle I have started. This research could measure the current status concerning e.g. organizational change frameworks, written risk assessment while downsizing, insider threat program, authorization conversations, access management, as well as education and training in terms of personnel security.
- Quantitative research that examines the cause and effect relationship between downsizing and the insider threat. Is there a causality, how strong is it, and how can the problem be treated?
- Master's or PhD study, performing a case study in a large Norwegian enterprise. This could include a field research, interviewing and observing managers and employees at all levels and departments of the given enterprise. Such study might measure or suggest improvements of frameworks and procedures for organizational change in terms of the insider threat.
- White-paper on a best practice for mitigating the insider threat while downsizing in Norway.
- NorSIS, NSR, or other organizations, could conduct surveys providing quantitative data for future research within the field of personnel security management.
- I would welcome future master students to replay my study, questioning my findings or providing a different perspective.

Bibliography

[1] Chinchani, R., Iyer, A., Ngo, H. Q., & Upadhyaya, S. June 2005. Towards a theory of insider threat assessment. In *2005 International Conference on Dependable Systems and Networks (DSN'05)*, 108–117. doi:10.1109/DSN.2005.94.

[2] Standard. 2012. Societal security - prevention of intentional undesirable actions - terminology. NS 5830:2012.

[3] Probst, C. W., Hunker, J., Gollmann, D., & Bishop, M. 2010. *Insider Threats in Cyber Security*. Springer Publishing Company, Incorporated, 1st edition.

[4] Gollmann, D. 2011. *Computer Security*. Wiley, 3rd edition.

[5] Bishop, M. 2005. Position: "insider" is relative. In *Proceedings of the 2005 Workshop on New Security Paradigms*, NSPW '05, 77–78, New York, NY, USA. ACM. URL: http://doi.acm.org/10.1145/1146269.1146288, doi:10.1145/1146269.1146288.

[6] BusinessDictionary. 2016. Organization change. Last visited on 28 Sep 2016. URL: http://www.businessdictionary.com/definition/organization-change.html.

[7] Rørvik, R. & Nesheim, T. Nedbemanning og omstilling i store norske mediebedrifter: drivkrefter, trender, utfordringer. Technical report, SAMFUNNS- OG NÆRINGSLIVSFORSKNING AS, 2010.

[8] Freeman, S. J. & Cameron, K. S. 1993. Organizational downsizing: A convergence and reorientation framework. *Organization Science*, 4(1), 10–29. URL: http://dx.doi.org/10.1287/orsc.4.1.10, arXiv:http://dx.doi.org/10.1287/orsc.4.1.10, doi:10.1287/orsc.4.1.10.

[9] Greitzer, F. L., Kangas, L. J., Noonan, C. F., Dalton, A. C., & Hohimer, R. E. Jan 2012. Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. In *2012 45th Hawaii International Conference on System Sciences*, 2392–2401. doi:10.1109/HICSS.2012.309.

[10] IBM. Reviewing a year of serious data breaches, major attacks and new vulnerabilities. Technical report, IBM, 2016. URL: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEW03133USEN.

[11] Durbin, S. 2016. Insiders are today's biggest security threat. *Recode*. URL: http://www.recode.net/2016/5/24/11756584/cyber-attack-data-breach-insider-threat-steve-durbin.

[12] NSR. 2015. Kriminalitets- og sikkerhetsundersøkelsen i norge. *Næringslivets sikkerhetsråd*. URL: http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/Krisino/krisino_2015_utskrift.pdf.

[13] Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., & Rogers, S. Insider threat study: Computer system sabotage in critical infrastructure sectors. Study, U.S. Secret Service and CERT/SEI, 2005. URL: https://resources.sei.cmu.edu/asset_files/SpecialReport/2005_003_001_51946.pdf.

[14] Kowalski, E., Cappelli, D., & Moore, A. Insider threat study: Illicit cyber activity in the information technology and telecommunications sector. resrereport, U.S. Secret Service and CERT/SEI, 2008. URL: http://resources.sei.cmu.edu/asset_files/WhitePaper/2008_019_001_52266.pdf.

[15] Elmrabit, N., Yang, S. H., & Yang, L. Sept 2015. Insider threats in information security categories and approaches. In *Automation and Computing (ICAC), 2015 21st International Conference on*, 1–6. doi:10.1109/IConAC.2015.7313979.

[16] Colwill, C. 2009. Human factors in information security: The insider threat–who can you trust these days? *Information security technical report*, 14(4), 186–196.

[17] Beebe, N. L. & Rao, V. S. 2005. Using situational crime prevention theory to explain the effectiveness of information systems security. In *Proceedings of the 2005 SoftWars Conference, Las Vegas, NV*, 1–18. Citeseer.

[18] Clarke, R. V. G. 1997. *Situational crime prevention*. Criminal Justice Press Monsey, NY.

[19] Saathoff, G. B., Nold, T., & Holstege, C. P. 2013. Chapter 3 - we have met the enemy and they are us: Insider threat and its challenge to national security. In *Strategic Intelligence Management*, Akhgar, B. & Yates, S., eds, 24 – 35. Butterworth-Heinemann. URL: http://www.

sciencedirect.com/science/article/pii/B978012407191900003X, doi:http://dx.doi.org/10.1016/B978-0-12-407191-9.00003-X.

[20] Arbeidstilsynet. 2016. Act relating to working environment, working hours and employment protection, etc. (working environment act). English translation of Arbeidsmiljøloven (2005). URL: http://www.arbeidstilsynet.no/binfil/download2.php?tid=92156.

[21] Arbeidstilsynet. 2008. Omstilling? har du husket det viktigste? URL: http://www.arbeidstilsynet.no/binfil/download2.php?tid=98946.

[22] Tekna. 2015. Hovedavtale 2014-2016 mellom tekna – teknisk-naturvitenskapelig forening og nho – næringslivets hovedorganisasjon. URL: https://www.tekna.no/globalassets/filer/tariffavtaler/privat/nho/tekna-nho-hovedavtale-2014-2016.pdf.

[23] Akademikerne. 2016. Hovedtariffavtalen i staten (akademikerne). URL: https://www.tekna.no/globalassets/filer/tariffavtaler/stat/hta-akademikerne-staten-2016-2018-hovedtariffavtale.pdf.

[24] NHO. 2014. Basic agreement 2014 – 2017 lo-nho - with supplementary agreements. English translation of "Hovedavtalen LO–NHO 2014–2017 - Med tilleggsavtaler og NHOs kommentarer". URL: https://www.nho.no/siteassets/nhos-filer-og-bilder/filer-og-dokumenter/lonn-og-tariff/hovedavtalen-2014-2017eng.pdf.

[25] KMD. 2015. Personalpolitikk ved omstillingsprosesser. Ministry of Local Government and Modernisation. URL: https://www.regjeringen.no/contentassets/7156039a3bca445680f02fd7fd1c40bb/no/pdfs/personalpolitikk-ved-omstillingsprosesser.pdf.

[26] Hennig, T. 2011. Retningslinjer for omstilling i troms fylkeskommune. URL: http://ksysekstern.tromsfylke.no/docs/pub/dok00938.pdf.

[27] Ytreberg, K. 2014. Sjekkliste med risikovurdering omstillingsprosess. URL: http://ksysekstern.tromsfylke.no/docs/pub/dok02318.pdf.

[28] Lewin, K. 1947. Frontiers in group dynamics: Concept, method and reality in social science; social equilibria and social change. *Human Relations*, 1(1), 5–41. URL: http://hum.sagepub.com/content/1/1/5.short, arXiv:http://hum.sagepub.com/content/1/1/5.full.pdf+html, doi:10.1177/001872674700100103.

[29] Madsen, D. i., Klethagen, P., & Stenheim, T. 2016. *Innføring i organisasjon og ledelse*. bookboon.com. URL: http://bookboon.com/no/innfoering-i-organisasjon-og-ledelse-ebook.

[30] Keen, P. G. W. January 1981. Information systems and organizational change. *Commun. ACM*, 24(1), 24–33. URL: http://doi.acm.org/10.1145/358527.358543, doi:10.1145/358527.358543.

[31] Kotter, J. P. & Cohen, D. S. 2002. *The heart of change: Real-life stories of how people change their organizations*. Harvard Business Press.

[32] Kanri, H. 2017. More about hoshin kanri? Last visited on 05 Apr 2017. URL: http://www.hoshinkanripro.com/hoshin_kanri_explained.html.

[33] Kotter. 2017. 8-step process. Last visited: 2017-05-11. URL: https://www.kotterinternational.com/8-steps-process-for-leading-change/.

[34] Saksvik, P. Ø., Nytrø, K., & Tvedt, S. D. 2008. Sunn endring i organisasjoner. *Tidsskrift for Norsk Psykologforening*, 45(3), 295–300.

[35] Whitman, M. E. & Mattord, H. J. 2011. *Roadmap to Information Security: For IT and Infosec Managers*. Cengage Learning.

[36] Jünge, M. & Walters, S. Endrer nedbemanning den psykologiske kontrakten? hva skjer med de som blir igjen? Master's thesis, Universitetet i Stavanger, 2016. URL: http://hdl.handle.net/11250/2413090.

[37] Gandolfi, F. & Hansson, M. Jul 2011. Causes and consequences of downsizing: Towards an integrative framework. *Journal of Management & Organization*, 17(4), 498–521. doi:10.1017/S1833367200001413.

[38] Eliason, M. Uppsägningar och alkoholrelaterad sjuklighet och dödlighet. resreport, Institutet för arbetsmarknads- och utbildningspolitisk utvärdering (IFAU), 2014.

[39] Reiso, K. H. *Young unemployed, single mothers and their children*. phdthesis, Norges Handelshøyskole, 2014. URL: http://hdl.handle.net/11250/274524.

[40] Aagestad, C., Tynes, T., Sterud, T., Johannessen, H. A., Gravseth, H. M., Løvseth, E. K., Alfonso, J. H., & Aasnæss, S. 2015. Faktabok om arbeidsmiljø og helse 2015. *STAMI*.

[41] Mollestad, E. & Iversen, C. B. Nedbemanning og survivor syndrome: en casestudie av dagbladet. Master's thesis, Norges Handelshøyskole, 2008. URL: https://brage.bibsys.no/xmlui//bitstream/handle/11250/168083/1/Mollestad%202008.pdf.

[42] Verizon. Verizon 2016 data breach investigations report. Technical report, Verizon, 2016. URL: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

[43] CPNI. 2017. Advice. Last visited: 2017-05-12. URL: https://www.cpni.gov.uk/advice.

[44] UIO. 1998. Act relating to protective security services (the security act). English translation of Sikkerhetsloven (1998). URL: http://app.uio.no/ub/ujur/oversatte-lover/data/lov-19980320-010-eng.pdf.

[45] Nilsen, K. 2015. Sikkerhetsfaglig råd. URL: https://www.nsm.stat.no/globalassets/rapporter/nsm-sikkerhetsfaglig_raad_2015_web.pdf.

[46] Bishop, M. 2005. The insider problem revisited. In *Proceedings of the 2005 Workshop on New Security Paradigms*, NSPW '05, 75–76, New York, NY, USA. ACM. URL: http://doi.acm.org/10.1145/1146269.1146287, doi:10.1145/1146269.1146287.

[47] Bishop, M. & Gates, C. 2008. Defining the insider threat. In *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead*, CSIIRW '08, 15:1–15:3, New York, NY, USA. ACM. URL: http://doi.acm.org/10.1145/1413140.1413158, doi:10.1145/1413140.1413158.

[48] Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. Insider threat study: Illicit cyber activity in the banking and finance sector. Technical report, DTIC Document, 2005.

[49] Cummings, A., Lewellen, T., McIntire, D., Moore, A., & Trzeciak, R. Insider threat study: Illicit cyber activity involving fraud in the u.s. financial services sector. Study, Carnegie Mellon University, 2012. URL: http://resources.sei.cmu.edu/asset_files/SpecialReport/2012_003_001_28137.pdf.

[50] Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T., & Flynn, L. Common sense guide to mitigating insider threats. Technical Report CMU/SEI-2012-TR-012, Software Engineering Institute, Carnegie Mellon

University, Pittsburgh, PA, 2012. URL: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=34017.

[51] CPNI. 2017. About cpni. Last visited: 2017-05-12. URL: https://www.cpni.gov.uk/about-cpni.

[52] CPNI. 2013. Personnel security risk assessment - a guide. URL: https://www.cpni.gov.uk/system/files/documents/46/06/Personnel-security-risk-assessment-a-guide-4th-edition.pdf.

[53] CPNI. Cpni insider data collection study - report of main findings. Study, CPNI - Centre for the Protection of National Infrastructure, 2013. URL: https://www.cpni.gov.uk/system/files/documents/63/29/insider-data-collection-study-report-of-main-findings.pdf.

[54] NSM. 2017. About nsm. Last visited: 2017-05-22. URL: https://nsm.stat.no/english/.

[55] Syvertsen, J. P. Insider threat. Master's thesis, Gjøvik University College, 2007.

[56] Arbeidstilsynet. 2017. Veileder om kontroll og overvåkning i arbeidslivet. Last visited: 2017-04-27. URL: http://www.arbeidstilsynet.no/binfil/download2.php?tid=260189.

[57] EU. 2016. Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). URL: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL.

[58] Government. 2017. Personvernforordning. Last visited: 2017-05-29. URL: https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/aug/forslag-til-personvernforordning/id2433856/.

[59] Coles-Kemp, L. & Theoharidou, M. *Insider Threat and Information Security Management*, 45–71. Springer US, Boston, MA, 2010. URL: http://dx.doi.org/10.1007/978-1-4419-7133-3_3, doi:10.1007/978-1-4419-7133-3_3.

[60] Sutherland, E. H. & Geis, G. 1949. *White collar crime*. Dryden Press New York.

[61] Martinko, M. J., Gundlach, M. J., & Douglas, S. C. 2002. Toward an integrative theory of counterproductive workplace behavior: A causal reasoning perspective. *International Journal of Selection and Assessment*, 10(1-2), 36–50. URL: http://dx.doi.org/10.1111/1468-2389.00192, doi:10.1111/1468-2389.00192.

[62] Posey, C., Bennett, R. J., & Roberts, T. L. 2011. Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security*, 30(6–7), 486 – 497. URL: http://www.sciencedirect.com/science/article/pii/S0167404811000630, doi:http://dx.doi.org/10.1016/j.cose.2011.05.002.

[63] Mishra, S. & Dhillon, G. 2006. Information systems security governance research: a behavioral perspective. In *1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference*, 27–35.

[64] Hadnagy, C. 2010. *Social Engineering: The Art of Human Hacking*. Wiley.

[65] Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. 2005. The insider threat to information systems and the effectiveness of iso17799. *Computers & Security*, 24(6), 472 – 484. URL: http://www.sciencedirect.com/science/article/pii/S0167404805000684, doi:http://dx.doi.org/10.1016/j.cose.2005.05.002.

[66] CPNI. 2016. Personnel security maturity model. URL: https://www.cpni.gov.uk/system/files/documents/c3/69/CPNI-personnel-security-maturity-model.pdf.

[67] NSM. 2015. Veileder i sikkerhetsstyring. Translated title: Guinelines for security management.

[68] CMMI. 2017. Capability maturity model integration (cmmi). Last visited: 2017-04-24. URL: http://cmmiinstitute.com/capability-maturity-model-integration.

[69] Traavik, K. 2016. Samhandling for sikkerhet - beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid. *Departementenes sikkerhets- og serviceorganisasjon*. URL: https://www.regjeringen.no/contentassets/03960058f3f94fbe9d290593bee22c1a/no/pdfs/nou201620160019000dddpdfs.pdf.

[70] Rich, E., Martinez-Moyano, I. J., Conrad, S., Cappelli, D. M., Moore, A. P., Shimeall, T. J., Andersen, D. F., Gonzalez, J. J., Ellison, R. J., Lipson, H. F., et al. 2005. Simulating insider cyber-threat risks: A model-based case and a case-based model. In *Proceedings of the 23rd International Conference of the System dynamics Society*, 17–21.

[71] Andersen, D. F., Cappelli, D., Gonzalez, J. J., Mojtahedzadeh, M., Moore, A., Rich, E., Sarriegui, J. M., Shimeall, T. J., Stanton, J., Weaver, E., et al. 2004. Preliminary system dynamics maps of the insider cyber-threat problem. In *Proceedings of the 22nd International Conference of the System dynamics Society*, 25–29.

[72] Ellison, R. & Moore, A. Trustworthy refinement through intrusion-aware design (triad). Technical Report CMU/SEI-2003-TR-002, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2002. URL: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=6581.

[73] Legg, P. A., Moffat, N., Nurse, J. R., Happa, J., Agrafiotis, I., Goldsmith, M., & Creese, S. 2013. Towards a conceptual model and reasoning structure for insider threat detection. *JoWUA*, 4(4), 20–37.

[74] Sokolowski, J. A., Banks, C. M., & Dover, T. J. 2016. An agent-based approach to modeling insider threat. *Computational and Mathematical Organization Theory*, 22(3), 273–287. URL: http://dx.doi.org/10.1007/s10588-016-9220-6, doi:10.1007/s10588-016-9220-6.

[75] Chabinsky, S. 01 2014. Reducing the insider cyber threat. *Security*, 51(1), 32. Opphavsrett - Copyright BNP Media Jan 2014; Sist oppdatert - 2014-03-06; United States–US. URL: http://search.proquest.com/docview/1504463700?accountid=12870.

[76] Costa, D., Albrethsen, M., Collins, M., Perl, S., Silowash, G., & Spooner, D. An insider threat indicator ontology. Technical Report CMU/SEI-2016-TR-007, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2016. URL: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=454613.

[77] Benjaminsen, T. Cyber-physical systems and the insider threat. Unpublished paper during masters course; Applied Information Security, 2015.

[78] Harkins, M. W. *The 21st Century CISO*, 139–153. Apress, Berkeley, CA, 2016. URL: http://dx.doi.org/10.1007/978-1-4842-1455-8_10, doi:10.1007/978-1-4842-1455-8_10.

[79] Benjaminsen, T. Ciso readiness for the next decade. Unpublished paper during masters course; Organizational and Human aspects of Information Security, 2016.

[80] Kowalski, S. 1994. It insecurity: A multi-discipline inquiry. *Department of Computer and System Sciences, University of Stockholm and Royal Institute of Technology, Sweden*.

[81] Benjaminsen, T. A case study of the telenor ss7 incident in 2016 from a socio-technical perspective. Unpublished paper during masters course; Socio-Technical Security Risk Modeling and Analyses, 2016.

[82] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. 2013. Internet of things (iot): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660. URL: http://www.sciencedirect.com/science/article/pii/S0167739X13000241, doi:http://dx.doi.org/10.1016/j.future.2013.01.010.

[83] NSR. 2017. Veiledning i bakgrunnssjekk. Last visited: 2017-04-25. URL: http://www.nsr-org.no/publikasjoner/veiledning-i-bakgrunnssjekk-article148-143.html.

[84] Vitnemålsportalen. 2017. Diploma registry. URL: http://www.vitnemalsportalen.no/english/.

[85] NSM. 2011. Håndbok i autorisasjon og autorisasjonssamtale. Translated title: Manual on authorization and authorization conversation.

[86] COSO. 2017. Welcome to coso. Last visited: 2017-05-25. URL: https://www.coso.org/Pages/default.aspx.

[87] COSO. 2004. Enterprise risk management - integrated framework - executive summary. URL: https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf.

[88] Leedy, P. & Ormrod, J. 2014. *Practical Research planning and design 10th edition Boston: Pearson New International Edition*. Pearson.

[89] Myers, M. D. et al. 1997. Qualitative research in information systems. *Management Information Systems Quarterly*, 21(2), 241–242.

[90] Barken, M. E. Fra brikke til ressurs en kvalitativt studie om arbeidstakers opplevelse av sosial støtte og kompetanseutvikling for trivsel på arbeidsplassen. Master's thesis, Universitetet i Agder; University of Agder, 2015.

[91] Malnes, R. 2012. *Kunsten å begrunne*. Gyldendal Akademisk.

[92] Boell, S. K. & Cecez-Kecmanovic, D. 2010. Literature reviews and the hermeneutic circle. *Australian Academic & Research Libraries*, 41(2), 129–144. URL: http://dx.doi.org/10.1080/00048623.2010.10721450, arXiv:http://dx.doi.org/10.1080/00048623.2010.10721450, doi:10.1080/00048623.2010.10721450.

[93] Cutcliffe, J. R. 2000. Methodological issues in grounded theory. *Journal of Advanced Nursing*, 31(6), 1476–1484. URL: http://dx.doi.org/10.1046/j.1365-2648.2000.01430.x, doi:10.1046/j.1365-2648.2000.01430.x.

[94] Taleb, N. N. 2007. *The black swan: The impact of the highly improbable*. Random house.

[95] A. 2017. Semi-structured interview a 25.01.17.

[96] B. 2017. Semi-structured interview b 27.01.17.

[97] C. 2017. Semi-structured interview c 30.01.17.

[98] D. 2017. Unstructured interview d 31.01.17.

[99] E. 2017. Semi-structured interview e 31.01.17.

[100] F. 2017. Semi-structured interview f 01.02.17.

[101] G. 2017. Semi-structured interview g 03.02.17.

[102] H. 2017. Semi-structured interview h 10.02.17.

[103] I. 2017. Semi-structured interview i 08.02.17.

[104] J. 2017. Semi-structured group interview j 13.02.17.

[105] Calder, A. & Watkins, S. 2008. *IT governance: A manager's guide to data security and ISO 27001/ISO 27002*. Kogan Page Ltd., 4th edition.

[106] Roer, K. & Petriĉ, G. Indepth insights into the human factor - the 2017 security culture report. Technical report, CLTRe, 2017.

[107] Leganger, C. 2017. Feilansettelser: - bedriften kan i verste fall gå konkurs. Last visited: 2017-05-09. URL: http://www.mediecom.no/2017/04/27/feilansettelser-bedriften-kan-i-verste-fall-ga-konkurs/.

[108] Jøsok, B. 2017. E-mail correspondence concerning comments by nsm on the results and suggested improvements.

[109] NorSIS. 2017. About norsis. Last visited: 2017-05-22. URL: https://norsis.no/english/.

[110] Malmedal, B. & Ulsrud, O. A. 2017. Unstructured interview of norsis 20.04.2017.

[111] Simonsen, A. R. 2017. About nsr. Last visited: 2017-05-22. URL: https://www.nsr-org.no/english/category172.html.

[112] Simonsen, A. R. 2017. E-mail correspondence concerning comments by nsr on the results and suggested improvements.

A Appendix: Interview Guide

Organizational Change

1. Does your organization have frameworks? Which standard? Share with me?
2. Experienced or planned org. change?
3. Risk assessment or threat assessment in org. change?
4. What is the key to success in org. change? From an org. perspective? From an employee's perspective?

Insider threat

1. How would your org define an insider threat?
2. How would your org approach the general insider threat?
3. Framework/program? In writing? Share?
4. Which controls do you have in order to protect against, detect, respond to, and recover after insider activity?
5. What are your thoughts on capability, motive and opportunity to launch an insider attack?
6. What are typical indicators of a malicious insider?
7. What are your thoughts on disgruntled vs dissatisfied employee? Norwegian term?
8. Do you conduct authorization conversations, in order to assess the employee's ability to handle a certain kind of information?
9. What are your thoughts on the dilemma whistleblower vs traitor?

Layoff Process

1. Give examples of why your org. must dismiss employees
2. How is notice given?
3. Notice time?
4. Severance pay?
5. Which controls and actions are implemented from employer before, during and after dismissals?
6. Guidelines and training concerning management and legal?

Research question 1

1. How do Norwegian organizations approach a downsizing in terms of the insider threat?

Improvements

1. Which improvements can be made in own organization's frameworks and processes?
2. Improvements in external frameworks or guidelines?
3. Important aspects for why a dismissed employee does not become a malicious insider?

Research question 2

1. How can the insider threat on dismissals be reduced through improved downsizing processes?

Wrap-up

1. Additional comments?
2. Questions I should have asked?