Exploring Cyber Incident Learning in Electric Utilities

Master's Thesis

MSc Crisis and Security Management

Filip Norén

Institute for Security & Global Affairs

Leiden University – Faculty of Governance & Global Affairs

Program: MSc Crisis and Security Management

Student ID: 2112523

Date of Submission: 13 January 2018

Word Count: 21,097 (excl. Appendices, References, and Transcripts)

Supervisor: Dr Wout Broekema, Assistant Professor, Leiden University

Second Reader: Dr Sanneke Kuipers, Associate Professor, Leiden University

Abstract

The threat of targeted cyber attacks against electric utilities was showcased in its most dramatic fashion yet in the 2016 Ukraine attack, but power grids also remain vulnerable to more common cyber incidents. Meanwhile, many methodologies on cyber incident response include 'follow-up' phases that stress 'lessons learned,' but they omit advice on how organisational learning from incident might be achieved. The wider importance of incident learning for incident preparedness and response capabilities and, by extension, greater cyber resilience is clear in the case of power grids. The fall-out from a grid-down disaster could be catastrophic since practically all the fundamentals of society depend on electricity.

This study seeks to explore the factors that drive successful organisational learning from cyber security incidents in electric distribution companies. To shed light on this process, an exploratory study was designed to collect empirical data through semi-structured interviews with key industry experts. The findings in this study indicate that the most important factors in building a successful incident learning capability are organisational structure, organisational culture, senior management commitment, and regulatory pressure. As supporting factors, the individual traits of the cyber security lead, incident impact, internal lesson sharing, small-scale incidents, (mitigation of) organisational forgetting, and exercises were found to be important. These findings largely confirm the relevance of the existing incident learning body of knowledge, although suggesting a need to highlight the role of individual security leaders and regulations in stimulating incident learning.

Since electric distribution companies often have highly limited resources, owing in part to their unfavourable position in the smart grid transformation, this study provides a starting point for further academic research and theory-testing into the causal mechanisms underpinning the four key incident learning factors in greater detail. Equally, the findings constitute suggestions for managers of electric distribution utilities, consultants, and the industry more widely as to organisational changes that favour the incident learning process.

Acknowledgement

As the thesis-writing process comes to an end, and with it my time as a Crisis and Security Management student at Leiden University, a few words of thanks are needed. First, I would like to thank my supervisor at the Faculty for Governance and Global Affairs, Dr Wout Broekema, for managing to guide me while finishing his own doctoral thesis.

I combined my thesis research with an internship at Accenture the Netherlands. I want to thank everyone on the Security team for their support and always being ready to answer my questions. The professional environment was an important motivator. My gratitude goes first and foremost to my supervisor, Dennis van den Berg, for his devotion to giving me valuable feedback. A special mention goes to Bas Kruimer for teaching me much more about power grids than I could squeeze into this text. And my thanks to the other interns – Tamara, Jelmer, Javier, Basel & the TIBER boys – for excellent coffee company and emotional support.

Also, my heartfelt thanks to all the interview participants for sharing their knowledge and experience. This includes the numerous professionals – within Accenture and far beyond – whom I had important conversations with but did not end up interviewing.

Finally, I want to thank my family for their unwavering support. Extra thanks to my father for enthusiastically learning about new topics to be able to give me input.

… and should I ever float the idea of a PhD, can someone please remind me that my bucket list is full of exciting things that require no desk-sitting.

Filip Norén
The Hague
12 January 2019

Contents

1 INTRODUCTION

One week before Christmas 2016, a power outage struck the Ukrainian capital, Kyiv. Only some of its inhabitants were affected and the outage lasted only about an hour, yet this was no ordinary power cut. It was caused by the first ever malware framework purpose-built to remotely flip switches and cut off the power supply. It does so in a highly automated and scalable way, making it adaptable to power grids in wider Europe and North America (Dragos Inc, 2017). The attack was labelled Industroyer and CrashOverride by different researchers. What is genuinely alarming is the fact that researchers believe the 2016 attack to be a mere proof of concept. Any intrusion into an industrial network with systems using the same protocols should be thought of as a case of "game over" (Cherepanov, 2017, p. 15).

The Industroyer attack demonstrated that cyber attackers can and do target power grids. Targeted attacks were confirmed in the United States, Switzerland, and Turkey as of September 2017 (National Coordinator for Security and Counterterrorism of the Netherlands, 2018). The Industroyer malware showcases a capability that leverages knowledge of electric grid systems themselves. "It is not an aspect of technical vulnerability and exploitation. It cannot just be patched or architected away" (Dragos Inc, 2017, p. 3). If air gapping[1] and other architectural protections are not enough, electric utilities need to be proactive organisations that adapt their defences and incident management capabilities to evolving threats. Naturally, the question for energy grid operators as well as society at large is 'How can we best set up our organisations to defend against sophisticated targeted cyber attacks? How can we develop our incident preparedness and response capability to meet these threats?'

To highlight the need for organisational adaptation, let us turn to Ukrenergo, the Ukrainian energy company struck by the 2016 cyberattack. Half a year later, it was struck again – this time by NotPetya.[2] Ukrenergo had intended to implement new IT security controls, but they were too late. They had failed to learn from the Industroyer crisis (Greenberg, 2018). About half of IT security decision-makers often do not change their security strategy substantially, even after suffering a serious cyberattack, according to a recent poll commissioned by IT security firm CyberArk. The poll, involving 1,300 professionals across seven countries, points to a considerable "cybersecurity inertia" that prevents organisations from learning from past incidents, endangering business continuity (Ashford, 2018). By systematically identifying lessons from incidents, organisations can achieve meaningful organisational change and adaptation to improve their security posture and resilience. This is what Ukrenergo appears to have attempted, albeit not fast enough. This is what all electric utility companies would ideally do *when* they are affected by cyber incidents.

[1] See Chapter 2 for an explanation.

[2] NotPetya is a piece of malware that was originally deployed in Ukraine in June 2017, engineered to spread automatically, rapidly, and indiscriminately across the globe to achieve maximum destructive power, not financial or espionage goals. "The most devastating cyberattack since the invention of the internet," it crippled multinational companies and caused billions of dollars' worth of damage (Greenberg, 2018).

Organisational learning is a complex process, but it is important for the electric distribution industry and merits research.

"If this is not a wakeup call, I don't know what could be."

Security researcher Robert Lipovsky of security firm ESET on the indication that Industroyer seemed to be a dry-run (A. Greenberg, 2017).

1.1 JUSTIFICATION AND MOTIVATION

Many types of organisations seem to struggle with organisational learning from incidents. In particular, those organisations that, similar to electric utilities, operate industrial control systems often appear not to have systematic processes for learning from incidents (Grispos, Glisson, & Storer, 2017). There is little insight in academia on how cyber security incidents might drive organisational learning (Ahmad, Maynard, & Shanks, 2015; Shedden, Ahmad, & Ruighaver, 2010). Meanwhile, many methodologies on incident response include 'follow-up' or 'post-incident' phases that stress formal reports of lessons 'learned.'[3] For instance, the National Institute of Standards and Technology of the United States (2012, p. 38) holds that:

> "*one of the most important parts of incident response is also the most often omitted: learning and improving.*"

Standards and methodologies are typically limited to normative emphasis on learning from incidents and some technological aspects thereof. They are not instructive on how to leverage newly gained knowledge from incidents for wider organisational adaptation and development that feed into both preparedness and response for future incidents. Considering how organisations always face scarcity in resources and competing priorities, this thesis aims to shed light on what factors drive organisational learning from cyber security incidents in electric distribution utility companies.

1.2 RESEARCH QUESTION

This thesis takes an exploratory stance and poses the following research question:

What factors explain if lessons drawn from cyber security incidents are implemented in electric distribution companies?

[3] Some examples include NIST SP800-61 (Cichonski et al., 2012), ISO/IEC 27035-1:2016 (ISO/IEC, 2016), SANS (Kral, 2011), and European Network and Information Security Agency (Maj, Reijers, & Stikvoort, 2010).

To address the research question, the most important factors for incident learning are explored in semi-structured interviews with key industry experts. The experts' unprompted perceptions are solicited on what factors or conditions are most important when a DSO learns from incidents. Subsequently, the most prominent factors in the literature were used as conversation topics, aimed at evaluating *if* the experts agreed on their respective importance and *how* DSOs successfully leverage the respective factors for incident learning. The scope of the study is limited to the incident learning process of putting lessons drawn into practice to develop incident preparedness as well as incident management capabilities, all with a view to building greater organisational resilience in DSOs.

This study targets the process of learning from incidents at an organisational level rather than individual level, although the latter is a component of the former (Sabatier, 1987). The scope includes all types of cyber threats and incidents, but the main focus is on incidents originating in the corporate IT networks, whether the incident ultimately impacts grid control systems or not. This is because major cyber threats against grid operations typically originate in the corporate IT network, as seen with Industroyer (spear phishing) and NotPetya (ransomware). For the remainder of this paper, organisational learning from incidents will be shortened to incident learning. Likewise, cyber security incident will be shortened to incident. Electric distribution companies will be known by the acronym DSO (distribution system operator).

1.3 ACADEMIC RELEVANCE

Theoretical models for incident (and crisis) management are typically circular or include feedback loops, regardless of whether they relate to cyber crises or crises more generally. Examples include Jaatun et al (2009), Jaques (2007) and Line et al (2008). While the terminology differs between them, they share the concept of self-improvement over time. A similar feedback loop pattern features in (cyber) resilience models, such as Hollnagel (2011), Kayes (2015) and Kott & Linkov (2019). While the terminology used in these theoretical models differs somewhat, the underlying concept remains the same: continuous improvement. This indicates a recognised need for, and value of, learning from experience to improve future behaviour, expressed as a need to adapt, modify, or review.

In other words, learning – perhaps expressed as adaptation or evolution - is identified as a key component of cyber incident management frameworks as well as (cyber) resilience frameworks, but these frameworks do not provide theoretical tools to close these feedback loops and ensure organisational learning. Therefore, this study explores organisational learning from (cyber security) incidents as an instrument to ensure that incident experiences can inform the planning, preparation, detection, response, and recovery efforts that precede the revision phase. In so doing, this study also presents learning from incidents as a vehicle for strengthening the cyber resilience of organisations.

Moreover, little research has been done on aspects of learning from cyber security incidents, although notable exceptions include Ahmad et al. (2015) and Bartnes, Moe, & Heegaard (2016). In particular, the study by Ahmad et al (2015) is notable for introducing the Dynamic Security Learning (DSL) process model. It specifically concerns organisational learning from incident in a cyber security context. Although they make passing references to culture, they do not directly study

organisational factors or conditions that enable the steps in the DSL process, or any incident learning process, to take place. The present study, meanwhile, aims to do exactly that.

1.4 SOCIETAL RELEVANCE

This study contributes knowledge on how DSOs can organise themselves to leverage past cyber incidents in strengthening their ability to withstand cyber attacks with no impact upon power delivery. The societal relevance lies in helping DSOs establish best practices for implementing lessons drawn from incidents by exploring the incident learning process and examining it from the people and process perspectives rather than merely a narrow technical one. While technology may solve many incident preparedness, detection, and response problems, the preceding implementation of technology solutions may often itself be inefficient or fail due to people and process-related problems. Other critical infrastructure companies, especially those that operate industrial control systems, can also benefit. Through a deeper understanding of the conditions that enable successful incident learning, these organisations can improve their incident management and cyber resilience.

The wider importance of cyber resilience, and the organisational learning that underpins it, is perhaps never more apparent than in the case of power grids. The societal fall-out from a grid-down disaster is almost unimaginable. Practically all the fundamentals of society, including water and gas supply, food production and logistics, and sewage systems commonly depend on electricity. It is hoped that the findings in this study may help DSOs improve their preparation, planning and response to the now real threat of cyber attackers disrupting power grids.

1.5 READER'S GUIDE

Chapter 1 has introduced the research problem and research question, outlining the academic and societal relevance. Chapter 2 provides background on the electric utility industry to give an understanding of what the role of DSOs is. Chapter 3 provides a theoretical background on the organisational learning literature and theories, including a review of what factors and conditions have been found by researchers to influence incident learning. Chapter 4 explains the research design and introduces the methods used for data collection and analysis. Chapter 5 reports the findings of the study and discusses them with reference to the extant body of knowledge. Chapter 6 closes the study with conclusions and suggestions for further research.

2 BACKGROUND: THE ELECTRIC DISTRIBUTION INDUSTRY

This chapter provides a basic understanding of how power grids work and helps put the importance of cyber security and organisational learning into context. It paints a picture of the conditions that DSOs operate under and why DSOs are interesting to study.

2.1 THE BASIC COMPONENTS OF POWER GRIDS

The electrical infrastructures of societies today share their general structure as they consist of various components that perform the same task regardless of geography. There are some technical differences between power grids in North America and Europe, for example, not to mention other continents, but the basic layout is typically the same. Electrical infrastructure refers to the aggregate of components that makes up the power grid. In essence, a power grid has three stages: generation, transmission, and distribution, seen below:

Figure 1: Schematic of a traditional, centralised, unidirectional power grid (IER, 2014).

In the generation stage, electricity is produced from renewable or non-renewable sources in power plants. In the transmission stage, electricity is transported from power plants to local distribution grids through high-voltage lines, the backbone of electricity supply. Organisations operating transmission grids are known as transmission system operators, or TSOs. In the distribution stage, electricity is delivered from the transmission lines to the end-user by 'stepping down' or reducing the voltage using transformers. Depending on the country or regional jurisdiction, some distribution companies also charge end-customers for their electricity use, acting as energy retailers as well. Organisations operating distribution grids are known as distribution system operators, or DSOs.[4]

[4] It serves to briefly explain the 'DSO' abbreviation used throughout this paper. The long-standing term for an organisation operating a power distribution grid has been distributed network operator, or DNO. DSO reflects the shift from a unidirectional grid that merely delivers energy that has been generated in a limited number of locations to dispersed consumers to a grid where electricity is consumed and generated in a decentralised, flexibility and unpredictable manner through small-scale power plants, such as solar panels and electric cars. The S in TSO reflects an associated shift from the previous TNO term (Accenture Strategy, 2016).

2.2 THE ROLE AND CHARACTERISTICS OF DSOS IN POWER GRIDS

This study focusses on DSOs rather than TSOs within the electrical infrastructure because the latter have so far received more attention with regards to security. On account of their market role and technical realities, operations in transmission are more automated than in distribution, and they often have more resources to spend on emergency (incident) response and maturing their security capabilities (Accenture, 2017).[5] Hence DSOs are considered more important as objects of inquiry.

Akin to many critical infrastructures, all stages in the power grid rely on operational technology, or OT, defined as "hardware and software that detect or cause a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise" (Gartner, n.d.). A major segment within OT is industrial control systems, or ICS, which can be used to monitor and control industrial processes, such as power consumption in a grid. ICS can operate virtually in real-time and allow for significant process automation, improving efficiency while reducing cost (Kargl, Van Der Heijden, König, Valdes, & Dacier, 2014). As professionals, OT engineers have typically been trained to prioritise those technical and commercial aspects. To achieve these objectives through data-gathering, analytics and optimisation, control systems are interconnected with the corporate IT network and the internet to ever-increasing extents. Air gapping IT and OT (when possible) lets staff put faith in the security of their equipment, but there is no such guarantee.[6] All organisations using OT/ICS rely on third-party tools and providers to some degree, which results in the use of remote maintenance links or external staff visiting sites to physically connect their devices (laptops, USBs, etc). Likewise, the DSOs' own staff may connect their devices for diagnostics or repairs. These acts put the OT systems in danger since a backdoor is effectively opened to outside attackers, either in the organisations' IT networks or on the internet. Cyber security threats against OT (grid operation) often originate in the corporate IT network, as seen with Industroyer (spear phishing) and NotPetya (ransomware).

As such, DSOs are fundamentally characterised as engineering and physical operations organisations. Consequently, a certain organisational divide emerges between IT and OT departments and staff. This is in many cases both natural and necessary as these departments have contrasting roles and priorities. For example, relay stations in the Netherlands require DOS-based software, which any given IT department has not dealt with for at least 20 years. Cyber security for OT should be a key concern for DSOs, in addition to the pressing cyber security needs regarding their corporate networks, similar to any organisation.

[5] Further supported by personal conversations with ICS security consultants within Accenture.

[6] "[An] air gap in cyber security refers to a situation in which a sensitive computer, classified network, or critical infrastructure is intentionally isolated from public networks such as the Internet" (Guri & Elovici, 2018). While air gaps are useful and tend to make an attacker's task harder, the fallacy of trusting an air gap to guarantee data security has been conventional wisdom for many years (Byres, 2013).

2.3 ACTIVE CYBER THREATS AND NEW ATTACK SURFACES

"The grid is still getting hit."

Alex Orleans, analyst with cyber security company FireEye (Hay Newman, 2018).

What makes the cyber security of DSOs alarming is the active cyber threat landscape. For instance, there is reportedly a concentrated cyber espionage campaign aimed at the U.S. electrical grid by a Russia-linked group commonly known as Energetic Bear or Dragonfly 2.0. The group distinguishes itself through patience, determination, and methodicalness. It has targeted European energy utilities and ICS operators in the past (Hay Newman, 2018; Symantec Corporation, 2014). In the case of the U.S., a set of resilience and defence baselines known as NERC CIP,[7] inspired by weather-related blackouts in 2003, have helped spread best practices for network defence. However, these regulations only apply to generation and transmission companies, which have hardened their systems accordingly, but they are not a requirement for distribution. A key nuance is that the actions of these threat actors are likely not primarily aimed at triggering large-scale blackouts – while they may potentially possess that capability, as seen in the 2016 Ukraine incident – but of traditional intelligence-gathering. While the chief alleged culprit above is Russia, China has a long-standing interest in industrial espionage in the West. Additionally, Iran is increasingly emerging as an actor, most recently with the surgical, well-resourced SamSam campaign against mainly public services, such as hospitals, in the U.S., Europe, Australia, and Israel (Accenture, 2018; Symantec Corporation, 2018).[8]

Along with active threats, the attack surface of electrical systems is growing on the back of the so-called smart grid transformation. The smart grid is simply the electrical grid enhanced by IT that notionally turns it into an 'intelligent' network. This transformation matters for cyber security in DSOs because it involves the increasingly widespread use of distributed energy resources (DER). They are small generators, such as solar panels, that tend to be located at end users' homes or businesses, generating energy that can be used on site when needed and fed back into the distribution grid when not needed. DER devices tend to be connected to the internet, where they effectively increase the attack surface and provide potential points of compromise for an adversary wanting to destabilise a distribution grid. The role of DSOs in the market as part of the traditional unidirectional electric infrastructure in Figure 1 means that DER also infringe on DSOs' revenue model, putting additional pressure on their budgets. The insertion of energy into the grid for profit (albeit modest for now) may ultimately prevent DSOs from collecting sufficient revenue to offset their fixed costs for providing reliability in supply of energy, for which cyber security is a growing budget post. Given these developments in threat actors and the grid itself, the need for DSOs to take cyber security for both IT and OT seriously will persist. Equally, these developments are an imperative for organisational learning from own incidents as well as those of peers.

[7] North American Electric Reliability Corporation Critical Infrastructure Protection
[8] Including the Netherlands, see Scholten (2018).

3 THEORETICAL FRAMEWORK

This chapter starts by reviewing concepts of organisational learning before defining organisational learning, incidents, incident learning, and lessons drawn with reference to the academic body of knowledge. It then discusses incident learning in ICS environments. The last section of the chapter presents key factors that the literature indicates will influence the incident learning process.

3.1 ORGANISATIONAL LEARNING FROM CRISES AND INCIDENTS

Before reviewing the literature on how organisations (try to) learn from incident experience, it serves to engage in some conceptual clarification of organisational learning. There are many definitions of organisational learning as some scholars see it as gaining new knowledge in a cognitive-only process, whereas others see it in the form of new organisational action. A third group conceptualises organisational learning as both cognitive and behavioural lessons (Argote, 2012; Fiol & Lyles, 1985; Schwab, 2007). The acquisition of new information is the first out of three 'steps' in the organisational learning theory by Argyris & Schön (1996). In the following steps, new information is processed to become knowledge, which is subsequently stored in an organisation. Drawing upon Crossan et al, who recognise how "cognition affects action (and vice versa)" (1999, p. 523), organisational learning is defined in this thesis as *the acquisition of new knowledge and the implementation of it to achieve more effective operation in line with organisational goals.* It is important to note that this definition recognises the importance of acquiring new knowledge in an organisation because this thesis focusses on the second part, the implementation of new knowledge to improve organisational action.

The body of knowledge on crisis-induced and incident-induced organisational learning is relatively small, probably owing to the fact that the crisis management discipline is comparatively young (Penuel, Statler, & Hagen, 2013). As a concept, crisis learning is often concerned with public organisations, government agencies, or government's role in crisis coordination. The overarching recurrent theme in public organisations regarding learning from crises and disasters is that it is difficult and tends to be inefficient or uncertain, or fail altogether (Smith & Elliott, 2007). Some exceptions in which public bodies were found to have successfully learned from crises include van Duin (1992) and Broekema et al (2017). By contrast, incident learning is more influential in the safety management literature spanning both private and public organisations. The two are logically connected since an adverse event that may be called an incident in a defined space can easily expand into a crisis in our interdependent, interconnected world. The incident learning literature is often concerned with safety incident management rather than security and resilience. This thesis takes the view that the body of work focusing on *safety* incidents is relevant for the study of *security* incidents because they share many themes, such as problems in drawing appropriate lessons to be learned and ensuring that those are implemented. This assumption is supported by the literature review by Line & Albrechtsen (2016) into theory and practice within industrial safety management, investigating whether they may be applicable to information security incident management. The review concludes that the latter field can gain by borrowing from the former, academically as well as practically. This is based on the safety management field being more mature with longer traditions, there being more organisational research into industrial safety than cyber security to

date, awareness in individuals being greater for industrial safety risks, and employee participation being ensured by law in many instances (Ibid.).

3.2 INCIDENT LEARNING: THE IMPLEMENTATION OF LESSONS DRAWN

The first step in defining incident learning is to define an incident. The authoritative ISO 27035 standard holds that an incident is a "single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security" (ISO/IEC, 2016). In this paper, this definition is interpreted to cover both IT and OT incidents because adverse events in OT threaten key business operations in DSOs. The simplest definition of incident learning is perhaps organisational learning induced by cyber security incidents. Accordingly, incident learning corresponds to the acquisition of new knowledge and the implementation of it to achieve more effective operation in line with organisational goals. However, for the purposes of exploring the factors that influence the incident learning process together with practitioners, this definition needs to become sharper. A common term for the acquiring of new knowledge following an event, incident, or crisis is a 'lesson learned.' This term is characterised by its ubiquitousness across many (security) management fields, including cyber security. As evidenced by Tøndel et al.'s literature review into current practices for incident management, lessons learned are an established term in the academic cyber security community (2014). At the same time, it is a term familiar to practitioners (Cichonski et al., 2012; ISO/IEC, 2016). To exemplify, "the absorption of existing knowledge concerns for instance experience or lessons learned from others" (Drupsteen & Guldenmund, 2014).

It is important to note at this point that the research question uses the term 'lesson drawn' instead of 'lesson learned.' This is to avoid conceptual confusion as 'lessons learned' could be mistaken for a later stage in the incident learning process, automatically signifying that new knowledge was indeed implemented and positive organisational change was achieved. The term 'lessons learned' is often a misnomer in reality as organisations merely document new knowledge (acquiring it) rather than acted upon it and implementing it (Donahue & Tuohy, 2006). Lessons drawn can be diverse in terms of form and meaning as they are driven by organisational context, incident type, etc. In the post-incident phase when an organisation evaluates their response to an incident, lessons drawn are typically translated into improvement items. Improvement items are often divided into the people, process, and technology domains by practitioners and academics alike. The people, process, and technology domains within organisation management studies originated not within the IT sphere but developed out of Leavitt's 1964 article *Applied organization change in industry: structural, technical, and human approaches*. The simplicity and applicability of this triangle explain its continued use in research on both IT-related and non-IT-related organisational change. When the lessons drawn – the new knowledge acquired through the incident - are implemented, an organisation effectively institutionalises the changes suggested by this new knowledge (Ahmad et al., 2015; Crossan et al., 1999). As a result, organisational behaviour has now been changed to reflect new knowledge and incident learning has occurred. As such, one can define incident learning as the implementation of lessons drawn. By extension from the above, incident learning can be defined in more detail as *the enactment of changes to the organisation's operations across the people, process and technology domains as per the lesson drawn.* This definition will be used for operationalisation in Chapter 4.

3.3 INCIDENT LEARNING IN CYBER SECURITY AND ICS CONTEXTS

The preceding section provided the main definitions for this study. This section highlights the themes raised in the literature at the nexus between incident learning and ICS-operating organisational environments.

Grispos et al. (2017) find evidence that 'lightweight agile retrospectives' in the follow-up phase can be used for wider incident learning in ICS organisations. Retrospectives are originally a software development term, and refer to special meetings "to provide a lightweight approach to identify what worked and what did not work ... and use this information to reflect on and improve the processes used..." (Grispos et al., 2017, p. 63). Grispos et al find that even though retrospectives aid in lesson-drawing regarding incident response, few actions were taken to create wider learning from incidents, calling for further research as to why.

Recognising this problem, (Shedden et al., 2010) perceive that incident learning is often narrowly fed into the incident response process itself, wherefore organisations should incorporate double-loop learning into their incident learning activities. Double-loop learning theory is a long-established organisational learning theory by Argyris & Schön (1978). Effectively, they call for reflection on the underlying structures and governing variables for the broader incident preparedness and learning activities such that organisations can continuously improve their incident learning capacity. Shedden et al. make suggestions for incident learning strategies based on literature but do not test organisational factors that may drive this process (2010).

In response to the lack of understanding regarding incident response and learning in ICS environments, Line et al (2008) advance the Incident Response Management model (IRMA). In their view, IRMA "should also be applicable to other industries that rely on process control systems and integrated/remote operations" (Ibid., p. 244). Line et al. argue that IRMA puts emphasis on incident learning "both in a reactive and pro-active manner" (Ibid.). For the present study, a better understanding of the factors that drive successful incident learning will strengthen any organisation's capability for reactive as well as pro-active learning. What decides if the process is reactive or pro-active is the content of the lesson drawn. If it relates to the incident response system, it is reactive. If it relates to the wider incident learning system, it is pro-active. However, like Shedden et al., the IRMA model does not focus much on the underlying conditions that enable the incident learning process.

Similarly, Bartnes et al. (2016) conduct an in-depth study of Norwegian power distribution companies focussing on cyber exercises but they do not explicitly research the conditions that may drive the implementation of lessons drawn through evaluations. However, they make an important contribution in their recommendation that DSOs should *learn how to learn*. This concept is called deutero learning by Argyris & Schön (1996). Learning to learn effectively corresponds to the continuous development of one's incident learning capability.

In sum, this brief review shows that the factors that enable incident learning, whether 'narrow' or more wide-ranging, have not been offered much attention in the specific context of ICS and cyber security. Yet the authors indicate that these factors underpin incident management models and the

effectiveness of exercises. The following section presents factors that the literature suggests influence the incident learning process.

3.4 FACTORS FOR INCIDENT LEARNING

This section presents factors that academic research has found to influence incident learning. Works carrying out empirical research have been favoured despite the majority of literature on incident learning being conceptual or deductive (Drupsteen & Guldenmund, 2014). Also, access problems and a reluctance among practitioners to sharing incident data (Jaatun et al., 2009) are further reasons why studies concerning both private public organisations have been used to increase the available material.

3.4.1 Organisational Structure

Organisational structure decides the decision-making authority of an organisation, providing the 'connecting fiber' between its strategy and the behaviour of its people (Bowditch, Buono, & Stewart, 2007). The term refers to the formal configuration of individuals and groups concerning the division of authority, tasks, and responsibilities within an organisation (Greenberg, 2011). Organisational structure refers to formal reporting, determines what hierarchical levels there are, and what range of control managers have. It deals with grouping individuals into units, teams, and departments, and organising these with respect to the overall organisation. Also, organisational structure comprises the design of systems to ensure effective communication, coordination, and integration of effort across these sub-units (Child, 1984; Pfeffer, 1991).

There are three dimensions to organisational structure that inform the operationalisation of the concept in this study. These dimensions are complexity, formalisation, and centralisation (Robbins, 1990). Complexity is how labour and tasks are divided, such as the number of components (departments). There are two related concepts: Differentiation and Integration. Differentiation refers to the degree of segmentation of the organisation into components or sub-units. Integration is the quality of collaboration between departments as they work on task delivery. Differentiation can include the creation of temporary or permanent cross-functional teams (Bowditch et al., 2007). Formalisation is the extent to which an organisation relies on rules and procedures to direct member behaviour. Also, the degree of discretion in performing their tasks given to staff depending on their roles. Centralisation concerns decision-making authority; the level at which decisions are made, and whom is involved to what extent. While a centralised structure typically means that decisions are made by a few people at the top of the hierarchy, decentralisation entails the spreading of decision-making authority (low concentration).

Given the above, for the purposes of this thesis, organisational structure is defined as *the formal configuration of personnel into work units, the division of decision-making authority, tasks, and responsibilities between them, and the design of formal reporting mechanisms between them*. Organisational structure has been identified as a contextual factor that raises the probability of learning if it encourages innovativeness and reflective action strategy (Fiol & Lyles, 1985). A centralised and mechanistic organisational

structure leans toward reinforcing past routines, while an organic, more horizontal one fosters changes in beliefs and behaviours. Hence flexibility and decision-making structures are connected (Duncan, 1974). Meyer refers to organisational adaptation rather than learning,[9] but finds that "formalized and complex structures retard learning but that learning is enhanced by structures that diffuse decision influence" (1982, p. 533). Trim and Upton find that if a siloed structure exists, an organisation will learn slower and struggle to survive external crises. "The only cure for companies with a silo mentality is often a forced restructuring [which] witnesses the introduction of a number of new management policies" (Trim & Upton, 2013, pp. 121–122).

The *expectation* regarding organisational structure in this study is that, amid silos between IT security and OT and operations departments, the use of temporary delegations of tasks and decision-making authority are linked to more successful implementation of lessons drawn. The attribute that favours incident learning is the ad-hoc bestowing of accountability for the completion of a lesson drawn (improvement item) upon one or a few key individuals.

3.4.2 Organisational Culture

Organisational culture is a broad-ranging concept that has different meanings to different people in different organisations. One definition is the "system of shared values (that define what is important) and norms that define appropriate attitudes and behaviours for organizational members" (O'Reilly & Chatman, 1996, p. 160). Flores et al (2012, p. 641) identify four cultural antecedent (sub) factors within the literature. They are paraphrased below:

1. participative decision making: organisational members collectively clarify problems, plan corrective action, and evaluate their efforts, feeling that they are free to speak their mind.
2. organisational openness: the open communication and assessment of assumptions about the organisation and the environment it operates in, where the consulting of others is accompanied by the acceptance that conflicting views will exist.
3. learning orientation: recognising that individual learning is seen as conducive to organisational learning, the company has among its values a commitment to creating and using new knowledge and ideas, making these a priority and linking them to its future success
4. transformational leadership: proactive leaders who are charismatic, engage in develop the skills of subordinates, and encourage innovative problem-solving, helping to challenge established beliefs and appoint resources allowing the organisation to integrate, store, and institutionalise new knowledge.

Flores et al find that, overall, participative decision-making and transformational leadership exert the greatest influence on organisational learning, trailed by learning orientation and organisational openness. Additionally, an organisational culture of psychological safety, where employees feel safe to discuss incidents or shortcomings without fear of blame or sanctions, are likelier to learn from

[9] Meyer's definition of organisational adaptation is rather close to the definition of organisational learning used in this study.

experience than organisations whose members do not feel psychologically safe (Argyris & Schön, 1978; Edmondson, 1999).

For the purposes of this thesis, *organisational culture is defined as the values, habits and norms that guide members' behaviour in an organisation* (Flamholtz & Randle, 2014). Regarding the features of an organisation's culture that are linked to learning from incidents, Meyer found that a pluralistic organisational culture where authority was often delegated to ad-hoc groups for the solving of unfamiliar problems was conducive to organisational learning from adverse events (1982). Organisational trust can be considered a cultural concept that informs learning from cyber incidents because trust entails a climate of openness that makes people comfortable to report and discuss incidents without fear of blame (Drupsteen & Guldenmund, 2014). Evidence of a 'just culture' encourages and even rewards people providing incident information, which drives incident reporting, which in turn is a prerequisite for the learning process and implementation (Catino, 2008; Dekker, 2009).[10] Bartnes et al (2016) find that personnel perceive cyber security aspects as an extra burden in the form of cost, time and workload. Equally, DSOs give low priority to evaluations, not just after exercises, but after actual incidents because the operation and protection of the grid from physical damage takes priority.

In the above sources, some challenges associated with organisational culture and learning are faulty or insufficient reporting of incidents for reasons of fear and anxiety. Power struggles among staff and other political processes in the post-incident phase also hamper learning, as do secrecy and low transparency in the post-incident phase. In general, a risk of groupthink exists.

Expectation: Organisational culture is believed to be important because DSOs appear to still have clear identity distinctions between IT and OT environments, where teams working with one do not communicate well with the other, and both might treat security as an afterthought.[11] For example, in a general sense, they all agree that securing grid operations is a top priority, but in reality they have different values and beliefs as to what to prioritise. For OT engineers, grid reliability may be the top priority, while the IT department may consider the digitalisation of all work flows in the company as the top priority or puts GDPR compliance first.[12]

3.4.3 Incident Impact

The Incident Impact category draws heavily upon the concept of shared sense-making. It refers to the perception process through which an organisation and its members make sense of what caused an incident, what happened during the incident, and what lessons should be learned. Sense-making is key to returning to a state of normalcy through a creation of shared understanding of past events (Boin et al, 2005). Sense-making is used in this study as a synonym for information interpretation,

[10] According to Eurocontrol (2006, in Catino & Patriotta, 2013): "Within a just culture, frontline operators or others are not punished for actions, omissions or decisions taken by them that are commensurate with their experience and training. However, gross negligence, wilful violations and destructive acts are not tolerated."
[11] Personal conversations with Accenture consultants.
[12] GDPR is the European Union's data protection regulation, which put pressure on organisations to align their business processes and offerings with customer privacy requirements.

which is another term that is common in the literature for the process through which organisations make sense of new knowledge that they acquire and share internally.[13] Sense-making in this regard is important because it depends on the impact of an incident, the preferred term used by Drupsteen and Guldenmund (2014). Incidents that have a major impact are powerful motivators for individuals to draw lessons and create both cognitive and operational adjustments (Lampel, Shamsie, & Shapira, 2009). Bartnes et al (2016) finds that Norwegian DSOs saw no need to significantly improve their incident preparation because there had been no major attacks, but the 2014 Dragonfly attack created a high level of concern. Homsma et al. (2009) also find that a nexus between severity and time in the implementation of lessons, citing "a higher generation of new ideas and insights and a higher implementation of improvements in the week following the occurrence of the error." This is interpreted as a sense of urgency that fades quickly and reduced incident learning.

For this thesis, Incident Impact is defined as *the perceived severity of a cyber security incident, whether internal or external, by an organisation and its members in terms of physical, reputational and financial damage.* The associated level of emotion determines the degree of concern shown by employees for implementing lessons drawn. Note that external incidents that occur in other DSOs are included in this definition as information-sharing platforms for energy utilities exist in addition to traditional and industry-specific media channels.

Expectation: Incident impact will be important in DSOs because an incident that is interpreted as minor by many staff, e.g. it only affected the business IT network, would probably not influence them to put additional effort into implementing lessons drawn. By contrast, if the attack reaches OT, e.g. causing a substation to shut down, the sense of urgency would drive incident learning.

3.4.4 Senior Management Commitment

Senior management commitment to incident learning is believed to be a key factor in enabling the implementation of lessons drawn. The author has chosen to include both executives and board members in this sub-section.[14] Senior managers often determine what actions are taken and how much investigation is done in relation to incidents. They should encourage investigations instead of just tolerating them (Kletz, 2008). For successful incident learning, long-term commitment and broad consistency in implementation are key factors (Donahue & Tuohy, 2009). All companies benefit from having security leaders who can translate security needs into business risk (Accenture, 2018). Top-level managers are intimately tied to organisational culture in cyber security contexts (Trim & Upton, 2013). They have the most power to make sure that the organisation's values include embracing change. It is less likely that staff lower down the hierarchy implement new processes. For instance, junior managers might believe it too risky to push for reformed procedures

[13] In the words of Flores (2012): "Information interpretation helps reduce equivocality and thus is critical in developing the shared understanding that leads to organizational learning (Daft & Weick, 1984)."

[14] The author recognises differences in other regards, see for example the 4i framework by Crossan (1999).

(Trim and Upton, 2013, p. 121). Accordingly, in this thesis, senior management commitment is defined as *the prioritisation by executives and board members of incident learning by enabling additional resources.*

The ear-marking of time and resources for building incident learning capacity requires commitment from managers. A willingness to do this has been shown to be an enabler for incident learning (Bartnes et al., 2016; Line et al., 2008). Also, they typically decide which junior staff oversee post-incident improvement projects. Involving employees who were directly affected by an incident in the post-incident phase when lessons are drawn has been shown to favour their implementation (Hovden, Størseth, & Tinmannsvik, 2011). Equally, when managers make sure that the incident learning process is a wide, interdisciplinary endeavour that involves employees from across the whole organisation, there is more effective execution of organisational change (Line & Albrechtsen, 2016; Schöbel & Manzey, 2011)

Expectation: Senior management commitment to incident learning is believed to be important because they can empower staff whom can translate complicated, technical operational processes into business language and security language. Therefore, they can make sure that incident learning takes place systematically.

3.4.5 Sharing Lessons Drawn

Among the various challenges to incident learning are both a reluctance to share incident-related information externally with industry and inadequate sharing of lessons internally between incident response teams and other functions within organisations (Shedden et al., 2010). Drupsteen and Guldenmund (2014) highlight the flow of incident information in a non-cyber security context. Line and Albrechtsen (2016) highlight how information should flow in a systematic manner beyond response teams to include larger parts of organisations for learning to be effective. Lessons drawn tend to be available to a few individuals only, even though other parties could have use for them (Ahmad, Hadgkiss, & Ruighaver, 2012). A threat to organisational learning in this context is the risk of information overload when involving more people and providing everyone with more information (Lukic, Littlejohn, & Margaryan, 2012). To encourage cross-function communication and sharing of lessons, Shedden et al. (2010) propose to include informal perspectives in incident learning, including workarounds, informal networks and other unofficial activities. Muhren et al (2007) and Shedden et al (2011) illustrate that informal learning can be effective specifically for the response capability, but evidence shows that informal learning and practices can support formal learning in a wider sense (Shrivastava, 1983).

A particular vehicle for the sharing of lessons drawn within the organisation is the 'learning agency,' a dedicated group or even person collecting lessons and sharing them within the organisation to ensure that experience enters the organisation's memory (Argyris & Schön, 1996; Koornneef, 2000). Kolb (1984) adds that the staff of such an agency ought to be actively involved in the incident experience in order to gain genuine knowledge from it, for example by being actively involved in the analysis and investigation effort, aiming to tailor and share the lessons with other functions. Research by Bartnes et al. (2016) suggests that a cross-functional team can play such a coordinating role in the incident response phase.

For the purposes of this thesis, the sharing of lessons drawn as a factor for incident learning is defined as *the post-incident flow of information, formal as well as informal, that seeks to be systematic and reach beyond the work units that directly managed the incident.*

Expectation: The sharing of lessons drawn is believed to be important for their implementation in DSOs since these organisations often have organisational divisions between IT staff and grid operators, who have different perspectives and priorities but probably need to communicate and cooperate for lesson implementation. A cross-functional team focussed on sharing lessons and institutionalising them could help alleviate this, as could a greater focus on informal social networks.

3.4.6 Small-Scale Incidents

Hollnagel et al (2011) report that the use of near misses and minor mishaps for organisational learning is just as important as learning from 'fully-developed' incidents. More broadly, the crisis management literature describes 'incubation' (Turner, 1976) as the repeated dismissal of, or blindness to, relatively small signs (incidents or events) that suggest that a larger structural problem is afoot. Turner shows that recognising and acting upon such small incidents is imperative in avoiding large-scale crises. In an incident response context, Scholl and Mangold suggest that identifying and acting upon small security events and early warnings can prevent major incidents and crises (2011). Learning from low-impact incidents seems not to be given priority (Ahmad et al., 2012). Koornneef establishes that there is untapped potential in the systematic learning from small-scale incidents, which is complex but can be realised. It is dependent upon the context of incident notification messages being known. A major problem is making small-scale incident learning cost-effective but having an internal learning agency can help (2000).

In this thesis, small-scale incidents and near-misses as a factor for incident learning are defined as *the company-wide recognition that small security events and the development of a systematic capability for implementing lessons drawn from them are crucial incident learning opportunities.* In their in-depth study of Norwegian DSOs, Bartnes et al (2016) find that none of the DSOs studied had a systematic approach to security metrics, such as a ticketing system for incidents: "Reports and registration could form a useful basis for evaluations, particularly in the absence of major incidents to learn from" (2016, p. 39). The post-incident review process tends to favour 'high impact' incidents rather than so-called 'high learning' incidents that can potential be more useful from a learning perspective (Ahmad et al., 2012).

Expectation: DSOs will recognise and target small security events and early warnings as a tool in their lesson-drawing process with the view to building a more cyber resilient organisation that can effectively prevent major incidents.

3.4.7 Organisational Forgetting

There appears to have been little interest recently in the concept of unlearning, popularised by Hedberg and contemporaries, in the 1970s and 1980s (Nystrom & Starbuck, 1984). A drastic

example of unlearning is the change of top managers *en masse* in a struggling company. Unlearning is described as a pre-condition for future organisational learning, but also a result thereof.

While unlearning is an active, premeditated 'loss' (shedding) of knowledge, there is also organisational forgetting. Defined by Broekema et al. in a public organisation setting as "the outflow of crisis expertise and experience" (2017, p. 336), it includes staff that leave for other opportunities, retirement, and internal restructuring. Broekema et al. found that previous crisis experience was needed to be able to draw lessons in the first place and that only parts of these could be retained within the organisation via plans and protocols. In this thesis, the definition of organisational forgetting is adapted from the above: *the outflow of individuals with cyber security incident management experience from an organisation.*

The *expectation* in this study is that unlearning can be used to jumpstart the incident learning process after major incidents. Organisational forgetting is expected to negatively affect incident learning capability, e.g. if younger, less experiences staff draw the wrong incident lessons because they lack the experience and OT knowledge of retired colleagues. The experience needed to set priorities for learning with regards to planning and preparation is therefore missing in the organisation, which guides the implementation (or dismissal) of incident lessons.

3.4.8 Exercises

The training of personnel in responding to incidents, as well as more general cyber security awareness campaigns, are important for incident learning. This section refers to both table top exercises, simulations and functional exercises (Grance et al., 2006). Experience with exercises and simulations among US state and federal agencies indicates that they "must be recast as learning activities targeted at improving performance, not as punitive tests where failure is perceived as threatening an organisation's ability to garner funding or maintain political favor" (Donahue & Tuohy, 2006, p. 18). Line et al. (2009) and Jaatun et al. (2009) argue that training sessions should be proactive and need further funding by OT/ICS-operating organisations. When people in an organisation are competing and a blame culture emerges, exercises can be used to diffuse this and show how it undermines the incident response capability and subsequent learning, according to Trim and Upton's (2013, p. 122). Bartnes et al find that "the lack of major incidents experienced by the [Norwegian DSOs that they studied] resulted in little focus or priority being given to training and exercises" (2016, p. 38).

In this thesis, Exercises as a factor for incident learning is defined *as the systematic staging by an organisation of periodic table top exercises and functional exercises concerning cyber attacks on the IT network.*

Expectation: Exercises serve as a factor for incident learning in that they create a sense of urgency since participants find them challenging and find that, even if they have plans and procedures in place, their readiness is worse than they believed. As such, exercises and simulations essentially function as 'eye openers' for the need to implement lessons drawn from previous (and future) incidents.

4 METHODOLOGY

This chapter outlines the methodology used in addressing the research question. Motivations are given for the choices made with regards to the methodology and overall research design. Finally, certain issues regarding confidentiality are discussed along with an analysis of the trustworthiness of the research design.

4.1 RESEARCH DESIGN

To address the research question, a qualitative, exploratory research design was devised (Denzin & Lincoln, 1994; Stebbins, 2008). It uses a single unit of analysis: the incident learning *process*. The unit of observation is at the individual level: the experiences of nine key experts with insight into successful incident learning. The data source is the key experts' combined experiences from numerous DSOs. Since the primary aim is to explore factors that explain if incident learning is successful, it was deemed appropriate to study the incident learning process by focussing on experiences of positive, successful incident learning, i.e. an outcome-driven approach (Haddon, 2012). The study seeks to understand differences between incident learning factors rather than a process of change, i.e. not directly measuring the incident learning outcome caused by each factor (Bourque, 2004). Accordingly, this study seeks to make relatively passive or tentative causal inferences based on the findings, as opposed to a more rigorous causal study.

The choices underpinning this research design were guided by several practical considerations. Since there is little research on cyber incident learning, there seemingly were no pre-formulated hypotheses relating to industrial control system operators that could be tested, and the research environment limited the choice of methodology (Streb, 2012). Given the time frame for this thesis, it was deemed exceedingly difficult to secure deep-enough access to a (limited) number of DSOs to gather data from different sources and ensure internal validity. Confidentiality and sensitivity issues surrounding (cyber) security incidents make access to data needed for a causal study difficult. Examples include detailed incident reports and improvement plans tracking implementation of lessons drawn. Also, incident information is typically covered by non-disclosure agreements between clients and consultants. Additionally, vanishingly few of these companies have suffered serious cyber incidents (that are common knowledge). With the above in mind, it was deemed that expert interviews would satisfy the data requirement, especially as the aim is to explore the process of incident learning in an industry where it has rarely been examined, and regarding a type of incident (cyber) that is understudied.

4.2 OPERATIONALISATION

Independent and Dependent Variables

To study the conditions that are most conducive to incident learning, it is necessary to create indicators according to the concept definitions set in Chapter 3. An indicator is a qualitative factor that provides a simple and reliable means of detecting differences, improvements or developments caused by the independent variable upon the dependent variable in a particular context. (Kumar, 2010). The independent variables are the respective factors for incident learning and the dependent variable is incident learning. They are operationalised below in Table 1 and Table 2, respectively. The tables use abbreviations for incident learning and lessons drawn.

The dependent variable is incident learning, conceptualised as the successful implementation of a lesson drawn from an incident (Section 3.2). This study does not seek to outright measure incident learning because it is exploratory and outcome-driven, as described in Section 4.1. As such, incident learning is a static outcome rather than a dependent variable in the traditional sense. Therefore, no indicators were developed to measure the effect on incident learning of the respective independent variables. Rather, incident learning is defined along the three domains of people, process and technology, as introduced in Section 3.2. The purpose is for the reader as well as the expert interviewees to know what corresponds to successful implementation of a lesson drawn in this study.

Table 1: Operationalisation of the Dependent Variable

Operationalisation of the Dependent Variable			
Dependent variable	**Domains**	**Examples**	**Reference**
Successful implementation of lessons drawn: *the enactment of changes to the organisation's operations across the people, process and technology domains as per the lesson drawn* **Understood as a static outcome, see Section 4.1 and 4.2**	**People:** Change in roles & responsibilities or training to strengthen incident preparedness or response	A DSO appoints a CISO; trains OT engineers in cyber security skills	3.2**Error! Reference source not found.**
	Process: Change in (an aspect of) an IM plan, intended to strengthen incident preparedness or response	A DSO develops a detailed cross-functional internal communication plan for cyber incident response efforts	3.2
	Technology: Change in technical security controls, intended to mitigate vulnerabilities, harden devices, enhance incident response, etc.	A DSO improves IT/OT network segmentation, updates or reconfigures firewalls, patching, introduces a SIEM platforms etc	3.2

The independent variables are the respective factors for incident learning. Indicators associated with a particular factor are those features in DSOs that are present when the successful implementation of a lesson drawn is linked to that incident learning factor. The indicators were

developed using a deductive, creative process that involved asking the following questions: What indicates that [a certain incident learning factor] is linked to successful implementation of a lesson drawn from an incident in a DSO? What observable property or feature should an expert interviewee refer to for there to be concord between how they interpret a factor for incident learning in a DSO context and how the literature describes it?

Table 2: Operationalisation of the Independent Variables

Operationalisation of the Independent Variables			
Independent variables Section 3.4..	**Indicators:**	**Examples:**	**Interview Guide:**
Organisational Structure *the formal configuration of personnel into work units, the division of decision-making authority, tasks, and responsibilities between them, and the design of formal communication and reporting mechanisms between them*	**Integration:** collaboration between departments.	A DSO fosters collaboration between IT dept and OT engineers by assigning joint responsibility for an LD in an improvement plan (formal instrument)	8.2, 8.3.1
	Formalisation: (degree of) discretion given to managers responsible for implementing an LD	Formal inclusion of IT security staff in incident response plans; Special permission to ignore or develop SOPs given to a manager for the implementation of an LD.	8.2, 8.3.1
	Centralisation: the organisational level (ops, management, strategic/top) where the source of decision-making authority for implementation of LDs is located	Executives use top-down vertical command lines to realise their decisions on LD implementation.	8.2, 8.3.1
Organisational Culture *the values, habits and norms that guide organisation members' behaviour*	**Psychological safety** A social environment without fear of undue blame or judgement.	A manager can re-evaluate a previous decision not to prioritise IT security without fear of reprisal.	8.2, 8.3.2
	Flexibility in beliefs open communication and assessment of assumptions about the organisation and environment;	Operations manager and cyber security specialist explore disagreement regarding risk assessment	8.2, 8.3.2
	Participative decision-making: Non-managerial staff collectively bring up problems and help plan and evaluate solutions, feeling that they are free to speak their mind.	Operations staff being listened to about insecure maintenance procedures	8.2, 8.3.2
	Security mindset: Collective recognition that cyber security	DSO launches phishing training campaign for all staff; personnel perceive	8.2, 8.3.2

	awareness-building is (un)important.	cyber security as vital for operations	
	Promotion of cyber security by leaders: proactive top managers help challenge established attitudes and habits, putting resources toward cyber security	Proactive C-level executives champion the use of experience, i.e. implement cyber security LDs, as part of development of overall resilience plans	8.2, 8.3.2
Incident Impact *the perceived severity of a cyber security incident by an organisation and its members in terms of physical, reputational and financial damage.*	**Display of emotion** by staff in relation to incident; sense of alarm linked to impact	Staff express shock at the disarray caused by a data breach.	8.2, 8.3.3
	A spreading recognition that IL is needed across company departments	Staff in varying work units highlight the impact a data breach to ensure LD implementation.	8.2, 8.3.3
	A sense of urgency in implementing LDs	Staff express the need to quickly divert more resources (across PPT domains) to implementing LDs	8.2, 8.3.3
	External threat awareness related to incidents occurring in other DSOs, nationally and internally	Speedy implementation of an incident lesson learned by a foreign DSO	8.2, 8.3.3
Senior Management Commitment *the prioritisation by executives and board members of IL by enabling additional resources.*	**Empowerment** C-level supports junior/middle managers in implementing LDs	Emergency preparedness manager gets backing by CISO in reforming cyber IR procedures according to their first-hand experience	8.2, 8.3.4
	(Additional) budget for the investigation of cyber security incidents and the implementation of LDs	Budget approved for technical upgrades	8.2, 8.3.4
	(Additional human resources) for the investigation of cyber security incidents and the implementation of LDs	IL process is a wide, interdisciplinary endeavour that involves employees from across the whole organisation	8.2, 8.3.4
	Accepting time needed for the investigation of cyber security incidents and the implementation of LDs	Competing changes or projects in the organisation are postponed because of IL	8.2, 8.3.4
Sharing Lessons Drawn *the post-incident flow of information, formal as well as informal, that seeks to be systematic and reach beyond the*	**Routine** for sharing incident lessons	An IL working group gets routine updates on incident lessons	8.2, 8.3.5

work units that directly managed the incident.			
	Willingness to admit that an incident took place	Incident info is shared internally to spread employee awareness about cyber threats	8.2, 8.3.5
Small-scale Incidents *the company-wide recognition that small security events and the development of a systematic capability for implementing lessons drawn from them are crucial IL opportunities.*	**Feed mechanism** for implementing LDs from minor cyber security events into preparedness and response plans	A ticketing system is created for the reporting of minor incidents, which are periodically reviewed.	8.2, 8.3.6
	Recognition that small-scale incidents are additional opportunities for the DSO to learn		8.2, 8.3.6
Organisational Forgetting *the outflow of individuals with cyber security incident management experience from an organisation*	**Stranded projects** for implementing LDs	When an individual leaves a DSO, the organisation does not know how to complete an improvement item.	8.2, 8.3.7
Exercises *the systematic staging by an organisation of periodic table top exercises and functional exercises concerning cyber attacks on the IT network.*	**Inclusion** of LDs from exercises, implemented into preparedness and response plans	Debrief from a table top exercise turned into improvement items/projects	8.2, 8.3.8

4.2.1 Data Collection

The method used for data collection is semi-structured interviews. Nine interviews were carried out between early November and early December 2018. Most interviews were preceded by an initial conversation lasting about 15 minutes to establish that the potential key expert had insight into cyber incident response and post-incident learning in ICS environments, especially electric utilities. The ratio between introductory conversations held and actual interviews completed was about two to one. The interviews lasted between 45 and 60 minutes each and took place via Skype. Each interview was recorded to allow for transcription and systematic data analysis. The transcripts were made available with minor redactions to the first and second reader of this thesis at Leiden University to meet academic requirements. However, in keeping with the key experts' confidentiality requirements, the transcripts are not included in the published version of this thesis.

Identifying the Key Experts

The most common method used for identifying the key experts was LinkedIn. Most of the key experts were contacted through a cold email approach. The key experts who were interviewed are listed in Table 3. Some have technical backgrounds, including a few who still identify as 'coders' despite also working with 'bigger picture' issues, while others have administrative or regulatory backgrounds. The selection criteria were having a career working in ICS-operating organisations,

including DSOs' incident (or emergency) response capabilities, and having led or advised on post-incident learning activities. What unites and qualifies them as interviewees for this study is that they all have professional insight into post-incident activities and have experience with successful incident learning processes.

Using combinations of key words related to cyber incident response, emergency management, DSOs, and ICS cyber security, a surprisingly short list of potential key experts emerged. The selection of this line-up of key experts is partially based on availability within the time frame, but the author sought to be as systematic as possible by carrying out the above-mentioned initial conversations before the interview to ensure that the experts had suitable knowledge and experience.

The selection criteria were designed on purpose to fit both DSO managers and cyber security consultants. Both categories are represented among the key experts. This was done to broaden the pool of potential interviewees since the initial feedback was that many DSO employees were unwilling to share experiences relating to incidents, even though this study is designed not to require detailed incident data. Since the aim of the study is to explore the *process* of incident learning, it was deemed appropriate to collect data through consultants since they can draw upon experiences from numerous different companies. Importantly, the independent consultants in Table 3 have worked directly for DSOs in business resilience or emergency management roles as part of their professional backgrounds. Nonetheless, it is reasonable that professionals working directly for utility companies would not have the exact same perspective regarding successful incident learning as consultants. Each key expert's perspective bias is assumed to be (at least partially) offset by the mix of consulting and electric utility careers among the interviewees.

Table 3: List of Key Experts Interviewed

Name	Position or Experience	Company or Affiliation
Thomas C. Ryan	Grid Security Lead, former Emergency Management Lead	Accenture
Johan Rambi	Independent Privacy and Security Advisor, formerly of a Dutch DSO	Independent consultant with RambiCo
Ann Steeves	Emergency Management Expert for Energy Utilities, formerly of a U.S. DSO	Independent consultant, CEO of HC-EMI, LLC.
Donovan Tindill	ICS Cyber Security Senior Consultant, IEC/ISA standards contributor	Global industrial cyber security vendor & consultancy
Key Expert 5	OT Cyber Security Engineer, standards developer/editor for the IEC	Mediterranean DSO
Key Expert 6A & 6B	Red Team Lead & Incident Response Lead	Accenture
Dean C. Desautels	Emergency Planning Manager	Eversource Energy[15]
Clint Bodungen	Executive VP for ICS Cyber Security	LEO Cyber Security[16]
Ernest Hayden	ICS Cyber Security Consultant, former DSO employee	Independent consultant

4.2.2 Interview Guide

The structure of the interviews is detailed in the interview guide in Appendix A. The guide reflects the research design as it starts with an exploratory part. The second part is linked directly to the incident learning factors suggested by the literature in Chapter 3. This interview structure has the merit that it lets the interviewer elicit the experts' experiences of incident learning from different directions. If the expert brings up a certain factor by themselves in the exploratory part, it may be further dissected in the explanatory part. If the expert does not bring a certain factor by themselves in the exploratory part, the reasons as to why may be further dissected in the second part.

Since the interviews are semi-structured, this guide is not followed in minute detail. The amount of time spent on each question and the order of the questions may differ from interview to interview, while follow-up questions may be added if the interviewee's replies lend themselves to it. The philosophy underpinning the interviews is to explore the factors driving incident learning processes in an interactive manner. The guide was designed to let the experts do most of the speaking while avoiding a scripted and mechanical feeling. The purpose of the guide is to provide

[15] The respondent speaks as an industry professional. He does not speak for Eversource Energy in any official capacity.
[16] The respondent speaks as an industry professional. He does not speak for LEO Cyber Security in any official capacity.

context and ensure that all key topics are covered in the conversation (Kvale & Brinkmann, 2009). As such, the interview guide is meant to turn the interviewees into participants in the study rather than mechanical answering machines (King, 2004). Neither the interview guide nor the research question refers specifically to 'organisational factors' because it encourages each interviewee to report their understanding of empirical reality more freely and accurately, without consciously or unconsciously changing their replies to fit the word 'organisational.' Rather than making the findings arbitrary, this fits the study's exploratory aims.

4.2.3 Data Analysis

After transcribing each interview, latent content analysis was carried out using NVivo 12. The transcripts were coded sentence by sentence or paragraph by paragraph against the indicators presented in Section 4.2. The analysis followed a two-step procedure. The first step used a directed content analysis approach (Hsieh & Shannon, 2005) and consisted of interpreting the key experts' answers pertaining to the initial, open-ended questions in Section 8.2 of the Interview Guide. Each new factor or condition that the key experts brought up as most important for incident learning was matched to the indicators or given its own category. These categories are called nodes in NVivo. After interpreting all transcripts, each node was opened to view an organised list of all references to that particular incident learning factor from all transcripts, as shown in Figure 2. This allowed for a thorough re-reading of the experts' perceptions regarding each node. Frequently, the experts would refer to several factors or conditions in the same sentence or paragraph, in which case the sentence or paragraph was coded into all applicable nodes for analysis.

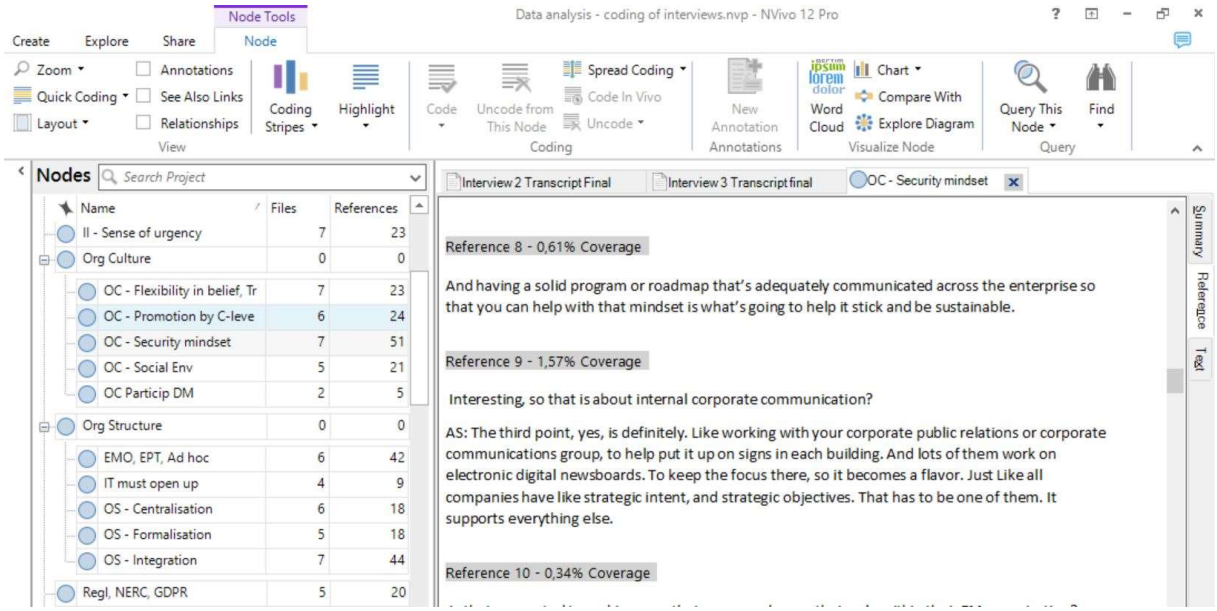

Figure 2: Screen dump showing interpretative coding and analysis

The analysis of the relative importance of the incident learning factors raised by the experts was an interpretative process carried out with three aspects in mind. First, when key experts identified a given factor as most important or critical for successful incident learning, this was recorded. Second, the frequency of experts' references to the respective factors was noted. Third, when certain factors would appear as vital in experts' arguments pertaining to other factors (Section 8.3), this was interpreted as raising the importance of those factors. Contradictory statements given by the experts regarding the importance of a given factor were resolved by interpreting what the majority view was, also considering the whole of the dissenting experts' transcripts and if any feature of their professional backgrounds and experiences would lead them to be obviously biased.

In the second step, the interview data associated with the factor-specific explanatory questions in Section 8.3 was analysed. The indicators developed above were used interpretatively to determine why each factor is important for incident learning by establishing what causal mechanism the experts' perceived as critical between a post-incident action item being made and it becoming operational reality for the company going forward. The indicators are essentially detecting which causal mechanisms, as informed by the literature, that experts perceive to be most important. In a handful of instances, an expert did not perceive a clear link between a certain incident learning factor and the successful implementation of lessons drawn. These instances were judged to lower the relative importance of a given factor. These cases were exceptionally rare, however, as there were no apparent patterns between those cases in terms of what factor they concerned or what the context was. Therefore, no specific comments have been made towards them in Chapter 5.

The absence of any of the indicators in any of the eight factor-specific discussions, defined as the impossibility of coding it, was also considered valuable. The conditions or themes that the key experts brought up instead were interpreted using a general inductive approach inspired by David Thomas (2006). This approach is data-driven in that it uses "detailed readings of raw data to derive concepts, themes, or a model through interpretations made from the raw data" (Ibid., p. 238). This is suitable to the purpose of this thesis as it involves the identification and definition of categories or themes after multiple readings of the raw data – similar to *in vivo* coding.

The findings are presented thematically according to the order of the tentative factors for incident learning. For each factor, the findings related to the first (exploratory) step and the findings from the second (explanatory) step are presented together.

4.2.4 Confidentiality

All recordings, transcripts and any interview notes were stored securely and deleted once data analysis was completed. Due to the potentially sensitive nature of incident experiences shared by the experts, the interview transcripts are not included in the final version. Verbal consent was obtained to record all key experts. For the sake of accuracy, the findings were sent for review to each key expert to ensure that any quotes were correctly attributed, and no misunderstandings had occurred. No expert found reason to withdraw consent. One expert suggested a few changes to quotes attributed to them to clarify their points. These changes were accepted. Those key experts whom appear with full names have given their explicit consent.

4.3 TRUSTWORTHINESS

Research is often assessed in terms of validity and reliability. Validity refers broadly to "the appropriateness, quality and accuracy of the procedures you adopted for finding answers to your research questions"(Kumar, 2010, p. 166). Reliability refers to the consistency and stability of a research instrument when it is used repeatedly, and thus predictability and accuracy of the findings (Kumar, 2010, p. 169). There is a debate as to the suitability of these assessment terms when it comes qualitative research. In essence, the debate is concerned with whether it is even possible to ascertain the ability of qualitative research instruments to measure what they are expected to and how consistent they are when the data collection questions are neither static nor completely structured (Kumar, 2010, p. 171). This study adopts the approach of Trochim and Donnelly (2006) who argue for the use of *'trustworthiness'* in qualitative research. Trustworthiness is determined by four indicators: credibility, transferability, dependability, and confirmability, which reflect the validity and reliability of qualitative research.

The **credibility** criterion establishes whether the results of this study are credible or believable from the perspective of the participant in the research. Since this study explores the perceptions, experiences and beliefs of interviewees, they are best suited to judge whether the research findings accurately reflect their reality (Trochim & Donnelly, 2006). Therefore, the findings were sent to the respective interviewees for comment. An issue in this regard is the fact that a more experienced research or skilled interviewer would perhaps be able to gather slightly different data and draw slightly different conclusions, yet the procedure of receiving feedback from the interviewees themselves somewhat mitigates this.

Transferability "refers to the degree to which the results of qualitative research can be generalized or transferred to other contexts or settings" (Ibid., p. 162). Trochim and Donnelly hold that transferability is primarily the responsibility of the reader who carries out the generalisation, meaning that it is their responsibility to judge whether the context and underlying assumptions can be transferred for their purposes.

Dependability is concerned with "the need for the researcher to account for the ever-changing context within which research occurs" (Ibid., p. 163), while **confirmability** refers to "the degree to which the results could be confirmed or corroborated by others" (Ibid.). A strategy for both is "to keep an extensive and detailed record of the process for others to replicate" (Kumar, 2010, p. 172). It has been an objective of this study to be exhaustive in this regard.

It serves to comment on extraneous variables, defined as other factors operating in a real-life environment that may increase or decrease the magnitude or strength of the relationship between independent and dependent variables (Kumar, 2010). As this thesis studies incident learning within large organisations with hundreds, or thousands, of processes, changes, and people at work at any given time, the isolation of extraneous variables is simply not possible. The use of follow-up questions in the interviews was aimed at gaining a deeper understanding of the respective factors to separate their influence from each other. In any case, the purpose of this exploratory study was not to measure causal effect but rather to indicate what factors may be fruitful objects for causal study in the future.

5 FINDINGS AND ANALYSIS

This chapter presents the findings that emerged from analysing the interview data. These findings reflect the importance of the respective factors for incident learning as perceived by experts when asked open-ended exploratory questions and when subsequently probed on the eight factors for incident learning introduced in Chapter 3. The experts identified four principal factors that are important when a DSO builds an effective incident learning capability: organisational structure, organisational culture, senior management commitment, and regulatory pressure. They stand out since they are significantly more prevalent in the data compared to the other factors. Two themes in the interview data, namely regulatory pressure and individual traits of the cyber security lead, could not be coded to existing indicators. Based on the underlying mechanisms described by experts when probed, these two themes would not have been a natural fit in any of the eight categories in the literature. Therefore, two new factors were created from these themes.

Reflecting these overarching findings, the four most critical factors are presented first, followed by the remaining six. After presenting the findings for each factor, links to the extant literature are discussed and sub-conclusions drawn. The key experts are referred to by their surnames whenever possible.

5.1 KEY FACTORS

5.1.1 Organisational Structure

The organisational structure of a DSO is identified as crucial for incident learning by most experts, particularly through two key structural aspects: the formalisation of an incident preparedness unit and formalised efforts at integrating the IT security department with other business units.

The formalisation of a preparedness unit allows for the creation of various case teams for specific incidents or categories of incidents. This ensures ownership of the learning process from lesson-drawing to the tracking of implementation according to a due date, suggested a majority of experts. Several North America-focused experts reported that many case team structures that they had observed were derived from the U.S. Department for Homeland Security's HSEEP.[17] The case team's success lies in that its composition is tailored to the type of incident. For instance, for a data breach in the corporate IT network, the most suitable business unit would be Governance, Risk and Compliance (or equivalent), while the most suitable individual to lead the team in executing on improvement items would be the Chief Compliance Officer (or equivalent). The team lead should be an executive or respected senior manager to ensure success because "no mechanism without a leader, without someone who owns it, will last" (Rambi). The lead will typically assign responsibility for the process to a middle manager. The unit that is tasked to lead would also prioritise which

[17] "The Homeland Security Exercise and Evaluation Program (HSEEP) provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning." See https://preptoolkit.fema.gov/web/hseep-resources/improvement-planning

incident lessons are most important. Yet responsibility for incident learning is shared with other affected business units, wherefore these units should be represented on the team by a respected manager.

Since preparedness units are born out of, and operate through, documented, structured processes, they are evidence of considerable formalisation of the incident learning processes (Bowditch et al., 2007). Yet, they have ad-hoc aspects that provide flexibility, such as the team composition being incident-driven. Through the lens of Robbins' (1990) definitions of organisational structure, a preparedness unit would appear to technically increase organisational complexity by adding a functional unit, but without significantly increasing differentiation since case team members normally belong to other functions. Also, integration (quality of collaboration) would appear to benefit from case teams as they bring different business units together while maintaining clear links to senior management. In this sense, they appear to correspond with Bowditch et al.'s concept of cross-functional teams (Bowditch et al., 2007). Despite this clear link to, and ownership by, leadership, case teams represent decentralisation as decision-making regarding what lessons to draw and implementation plans originates with respective business units (Robbins, 1990). As such, the experts' perceptions are in line with Meyer (1982, p. 533), whom found that "learning is enhanced by structures that diffuse decision influence."

Another advantage of the preparedness unit as an organisational sub-structure is the suggestion by experts that it helps control the time factor (Homsma, 2009). There is a tendency for improvement items to lose urgency in the mind of managers and engineers, often referenced by the experts as 'blue sky work' replacing the incident. "The central organization needs to stay on top of this and mind the ship, asking what stage the remediation process is in – poking people" (Steeves). The preparedness unit is a tool to this end, findings suggest.

The second mechanism regarding organisational structure for incident learning is the building of (better) bridges between the IT department – and its security staff in particular – and virtually all other business units. A majority of experts suggest that an explicit strategy for the staffing of IT security and OT engineering staff such that they form personal bonds is a driver of effective lesson-drawing and implementation. Specifically, several experts highlight the need to stimulate or engineer one-on-one relationships for effective incident learning to take place. This takes the form of purposely staffing a 'smart cyber security specialist with a smart control engineer' on a project to implement a lesson drawn. The usefulness of this is described by Tindill:

> *"When they trust each other on an individual level, it is evidence that things have worked well. You start trusting the other to do their part - recognizing that the other person has special skills and a different set of priorities. If you can work with that, and leverage the IT security expertise, the plant is more reliable and more secure."*

This formalised 'social engineering' reportedly drives greater integration – the improved quality of collaboration – between IT and OT (Robbins, 1990). It would appear to help mitigate "silo mentality" between personnel and units that are, by virtue of their functions, siloed to a certain degree (Trim & Upton, 2013, pp. 121–122). Another mechanism for tighter integration that is worthy of mention is the report by one expert of observed success with creating a joint department for cyber security for both IT and OT. Given increasing internet connectivity, it has become more

critical to integrate the two from a security perspective. The creation of a joint unit favours incident learning through both structure and culture (Expert 5).

The expectations in Chapter 3 regarding organisational structure, i.e. temporary delegations of tasks and decision-making authority being linked to more successful incident learning, were mostly confirmed in the preparedness unit and its case teams. The bestowing of accountability for lesson implementation upon one or a few key individuals is a feature of the case teams, as described by the experts, while the usefulness of explicit one-on-one relationship-building was not covered by expectations.

5.1.2 Organisational Culture

The most important factor overall, organisational culture is identified as fundamental if lessons drawn from incidents are to be implemented by *all experts* without exception. In their collective experience, cultural transformation takes many years. DSOs should be proactive in achieving a *security culture* that is more conducive to incident learning. Tindill summed up the thoughts of many experts as follows: "Cyber security is not just a one-time investment that you implement, set, and forget. Cyber security is a program, it is a mindset." A must for such a proactive culture is executive buy-in: "You need to create a paradigm shift. You need to get executive leadership support conveying that we are one entity" (Rambi). Several components of security culture were widely referenced by the experts, as presented below.

Firstly, it was found that the use of a cyber risk management process – and indeed, cyber risk mindset – was linked to the establishing of a cyber security culture (e.g. Ryan; Tindill; Expert 5, Desautels). In the post-incident phase, it is common to have (at least) dozens of lessons drawn across the people, process and technology domains. A risk management approach helps determine which lessons mitigate the majority of the risk such that they can receive most resources. A risk management mindset among middle managers in IT and OT cyber security facilitates the necessary executive buy-in and is perceived by the experts as a driver for incident learning.

The second mechanism is the stimulation of an open, forgiving security mindset for the whole company, across all corporate functions. The experts brought up themes of cyber awareness, psychological safety, and self-reporting as the basis for this. Cyber awareness starts with the understanding that cyber threats against the organisation can target any of its employees, from linemen to CEO. Along with training for all staff on threats, such as spear-phishing and ransomware, the experts pointed to the merits of openness and lack of personal punishment for mistakes. Such a culture supports the post-incident mechanism as it drives a willingness and ability to report suspicious activity, if communicated well across the company. The experts generally perceived that a non-punishment attitude was encouraged in DSOs, but little to no attention appears to be paid to active encouragement mechanisms for individuals to report (potential) incidents, except for one instance shared by Johan Rambi (Catino, 2008; Dekker, 2009).

As the third component, trust between IT (security) and OT engineering and operations units was found to be both a challenge and an enabler for incident learning; trust in the sense that personnel in both units are working towards the shared goal of better protecting the DSO's operations,

despite conflicting priorities and viewpoints (e.g. Steeves; Tindill; Expert 5). This quote by Tindill helps illustrate this point:

> *"Historically, the control systems and IT groups do not trust each other, because they are so different. Control systems teams are inherently conservative as the potential consequences are high, and their security knowledge is lower. IT groups are much less conservative, they work on systems with lower consequences, and have more security knowledge."*

The finding reported above in the Organisational Structure section, highlighting personal trust on an individual level, recurs for culture in the interview data. To build trust, personal availability and dedication were found to be important. Several experts suggest that cyber security staff should preferably emulate OT engineers in that they are physically present on site, able to drop everything when needed to help solve a problem (Tindill; Expert 5). These findings suggest person trust helps create an environment where lessons drawn can be implemented with less tension.

It is worth highlighting, however, that differing priorities can be natural in DSOs. Bodungen explains the conflicts as follows: "If an incident does not threaten OT or there is not a precedent of it doing so, or a reasonable way to show it doing so, then OT [staff] do not care about it." This can be interpreted as natural because they prioritise operational reliability and efficiency, wherefore they will typically not tolerate downtime due to a remediations project related to the corporate network. As Bodungen emphasises, cyber security personnel must make a solid argument that there is unacceptable cyber risk to operations to motivate such an action. The problem can thus be said to shift to cyber threat intelligence.

Another aspect of organisational culture that was linked to incident learning capability is regional or national experience, according to most experts. "The cultural belief in some countries, where they look at their international relations, believe they are safe, and will not be the subjects of attacks, absolutely does affect security, and the ability to implement change" (Ryan). The most frequent example brought up by the experts was the United States, where incident learning was reportedly valued as relatively more important by DSOs.

With regards to the literature, these findings reaffirm the importance of transformational leadership – effectively cultural transformation from the top towards a security culture (Flores et al., 2012). Similarly, organisational openness (flexibility in beliefs) was an indicator that was frequently referenced by the experts. Conceptually, the idea of trust as presented above (and reported by the experts) appears, however, to be somewhat different from that used by Drupsteen & Guldenmund (2014). In their literature review on incident learning, they explain trust as a climate of openness that makes people comfortable to report and discuss incidents, which is reminiscent of what this study calls psychological safety. Therefore, organisational trust as found in this study, mainly between IT security specialists and OT engineers and operators, is understood more in line with Flores et al.'s idea of openness to opposing beliefs and a willingness to discuss them. As mentioned above, this trust is interpreted as helpful in relieving cross-function tension during lesson-drawing and implementation projects. Such projects often involve IT and OT directly or, more problematically, in indirect or poorly understood ways. Thus, it is reasonable that incident learning is favoured by deeper trust in the fact that colleagues from 'the other team' also have efficient and resilient delivery of electricity in mind.

The role of psychological safety as a driver for incident learning (as an aspect of a security culture), where employees feel safe to express ideas and raise problems without fear of blame or professional disadvantages, aligns with previous literature (Argyris & Schön, 1978; Edmondson, 1999). To achieve this, Ryan suggests striving for "a culture like the aviation industry, of self-reporting." The U.S. Federal Aviation Administration's Aviation Safety Reporting System has helped drive a culture where it is encouraged - and there is no penalty – when you say 'I made a mistake.' – both as a company and as an individual (Connell, 2004, p. 144). This could help drive improved internal lesson-drawing as well as external lesson-sharing to the benefit of particular DSOs and cyber security in the electric utility industry as a whole.

Both Bartnes et al (2016) and Jatuun et al. (2009) found differences in understanding of cyber security goals between IT staff and control system staff, which seem to be in line with the experts' perceptions. However, Bartnes et al. "did not identify any signs of mistrust between IT staff and control system staff" in their study into several Norwegian DSOs (2016, p. 41). "Rather than feeling mistrust, both IT staff and control system staff admitted the need for exchanging information and learning from each other to become better at both detecting and responding to incidents" (Ibid.). While this quote focusses on learning for the purpose of incident response in a narrower sense than the wider incident learning capability that this study primarily targets, the issue of trust affects both perspectives and the disparity of findings is notable. By contrast, Jaatun et al. (2009) did find such mistrust to be problematic. A potential reason for this discord is that the Norwegian DSOs studied by Bartnes et al. were reported as rather small, wherefore the IT and control system staff may have better chances at building personal confidence, whereas the experts interviewed for this study shared more generalised experiences from DSOs of varying sizes.

With regard to the expectation set in Chapter 3, the 'silofication' in cultural terms between IT and OT units was found to be a perceived challenge to incident learning. However, the findings appear to move beyond this expectation, as the pro-active building of an organisation-wide cyber security culture and mindset are also identified as the greatest enabler of incident learning in DSOs. The findings are inherently also a criticism of IT outsourcing. It appears that, to build trust and drive incident learning, cyber security knowledge should be available face-to-face, not on a support line to a different company or continent.

5.1.3 Senior Management Commitment

Having the explicit support from executive officers or board members is a major factor for successful incident learning, according to the experts, whom typically named it as most or second-most important. It appears that the higher up the support for an implementation project rests, the better its chances of sufficient resourcing and successful completion. The experts often cited the *impossibility* of running a meaningful incident learning process without the commitment of the executive or board-level. Regarding the indicators for senior management commitment, budget and empowerment were referenced three times as often as time or human resources, but that is likely since those two are ultimately also linked to financial considerations. Interviewees stressed that responsibility for implementation projects after incidents are often delegated to middle managers, such as an emergency preparedness manager chairing a case team.

Securing budget is challenging because of the seemingly abstract or intangible nature of cyber security. In the words of Ryan, "the future of technology and security is not capital – it is a cloud contract, or a virtual firewall, for example, which makes it more difficult to get the influence." Desautels raises a related concern: "A lot of IT is not capital improvement. You have to work extra hard to motivate and justify non-capital spending on IT or people-and-process fixes for cyber security in front of top managers."

These findings reinforce those by Bartnes et al., whose in-depth examination of incident learning in various Norwegian DSOs named "the extent of management commitment and the willingness to commit resources to facilitate learning" as key enablers of what they call "learning to learn" (2016, p. 41). Learning to learn is effectively what the continuous development of one's incident learning capability is. The delegation of responsibility for remediations projects after incidents to middle managers is consistent with the findings of Hovden et al. (2011) but the data cannot reasonably be used to comment on exactly which employees and departments should be involved in the incident learning process for it to be effective (Line & Albrechtsen, 2016; Schöbel & Manzey, 2011). The reason is that this exploratory study uses the incident learning process as the unit of study rather than the DSOs themselves, wherefore the data does not cover specific DSOs in sufficient detail.

The expectation that senior management commitment to incident learning would be important because they can empower staff who can translate complicated, technical operational processes into business and security language was not supported by the experts' perceptions. Rather, the experts' referred to empowerment in the sense of executives delegating power for incident learning projects to chosen managers and providing the necessary budget. It appears that a successful incident learning process starts with senior managers committing budget and people towards it owing to an (pre-existing) understanding that cyber security is vital to operations.

5.1.4 Regulatory Pressure

Regulatory pressure was referenced as a top-three critical factor for incident learning by a majority of experts. Therefore, it is included among the four stand-out factors. Regulatory pressure spurs continuous improvement even when there are no major incidents that demand attention. While regulatory compliance is typically a middle and top management concern, here it amounts to more than senior management commitment *per se* because regulatory pressure breeds – and ensures – senior management commitment. The interview data identified regulatory pressure as a driver when going from reactive to pro-active cyber security postures, as outlined in the Culture section. DSOs will start out seeking minimum compliance only because of internal resistance and having had regulation forced upon them in many cases, experts explained. After a few years, there is recognition that non-compliance itself is a business and operational risk, compounded in some cases by reputational concerns. As a result, DSOs' posture turns from a minimum compliance program to a bar that is set internally. "Non-compliance becomes less of a risk because you are not sitting on the edge of it all the time" (Tindill).

Some experts identified a lack of national or federal laws to accompany the industry-level rules and regional (or state) level laws that appear more commonplace. The pace-setters for regulation are

big organisations and industry associations rather than national governments. As one expert remarked, there are no widespread cyber security laws in all countries that mandate secure development and secure configuration at this time. Nonetheless, several North America-focused experts identify NERC CIP as a driving force for top-down attention to incident learning (for DSOs that also operate transmission). To paraphrase Hayden, if NERC CIP covered distribution companies, it could increase their improvement rate, including for incident response. Its forcing function as it has already driven improvement across the electric utility industry, which was mediocre in terms of cyber security.

However, the experts also pointed to several instances of negative regulatory pressure, which is when rules or laws impede other factors for incident learning (e.g. Tindill, Desautels, and Hayden). For instance, in several states across the U.S., state bodies have the ability to impose fines if they determine that a utility failed to properly prepare for, and respond to, any type of incident.

The process of establishing regulatory pressure as a theme in the interview data was organic and data-driven, as the experts made frequent reference to it and emphasised its importance. What was problematic was whether to create a new factor for regulatory pressure or consider it a sub-factor underpinning culture and senior management commitment. There are significant links between regulatory pressure and the other three stand-out factors. For example, top-down attention to an improvement item is a key enabler of its implementation. Regulatory pressure, or the quest for compliance, can fuel this commitment to incident learning. The experts emphasised the central role of regulation in pushing incident learning in DSOs that are immature in terms of cyber security as well as in more mature DSOs (e.g. Tindill; Hayden). In the latter case, current regulation is perhaps not enough for continued incident learning development. A more pro-active stance from industry as well as national governments, pushing governance requirements, would be needed. Nevertheless, this holistic influence on incident learning motivated the decision to name it a key factor.

5.1.5 Interconnectedness of the Key Factors

The analysis of the interview data found a striking interconnectedness between organisational structure, security culture, and senior management commitment. Consider, for instance, how structural features, such as the purposeful building of personal relationships between IT and OT units favours cultural aspects, for example open communication about operational assumptions in the organisation (Flores et al., 2012). Such a policy may require top managers' approval for additional manhours or temporary re-assignment of staff. Another example is how a preparedness unit serves to overcome divides between work units in terms of structure and culture. It allows for a short chain of command as well as considerable flexibility and delegation for the formulation of improvement projects (based on lessons drawn) to the analysts and engineers from the affected unit. This effectively amounts to participative decision-making (Flores et al., 2012). The strong link to executive decision-makers in case teams echoes the quantitative finding of Flores (2012) – expressed as transformational leadership - that senior management involvement is key for incident learning by the experts. Given how intertwined structure, culture and leadership are, these findings echo Meyer's finding that a pluralistic organisational culture where authority was often delegated

to ad-hoc groups for the solving of unfamiliar problems was conducive to organisational learning from adverse events (1982)

The intertwining of factors can also be seen in the case of risk management, a driving force in creating a security mindset across a DSO, according to the experts. It could be interpreted as a feature of organisational structure since a risk management approach demands documented work flows and processes. In this study, it was deemed to be, more than anything, a feature of culture because it is a mindset that influences the likelihood that cyber security and learning from incidents will guide the organisation's development. Arguably, however, it could also classify as a feature of senior management commitment because the risk management thought process is familiar to executives. They would be in the best position to champion it. It also plays a role in how effective a DSO is at learning from small-scale incidents.

It is perhaps surprising that the onus was commonly placed by experts on the IT and IT security units to open up to other business lines, in terms of more formal collaboration and communication. The opposite was not raised. This suggests that IT staff including managers might want to pro-actively build shared projects that let them interface with other lines of business to stimulate long-term incident learning.

With the above in mind, it might be instructive to think of the first three factors – structure, culture, and senior management commitment – as an incident learning triad in DSOs. The reasoning behind this term is that the remaining six subordinate factors can generally be tied back to culture, structure, and senior management commitment – occasionally also to regulatory pressure.

5.2 SUPPORTING FACTORS

The remaining factors, namely Individual Traits in the Cyber Security Lead, Incident Impact, Lesson-Sharing, Small-Scale Incidents, Organisational Forgetting, and Exercises, have a common denominator in that they were predominantly perceived as sub-factors to the four principal factors by the experts interviewed. They are presented and discussed in order below.

5.2.1 Individual Traits of the Cyber Security Lead

The role of the individual cyber security leader and their credibility within the DSO is a major theme in the data. Having an influential leader for cyber security, such as a Chief Information Security Officer (CISO), is key to being able to leverage people and budget within the organisation. To paraphrase Bodungen, a board that is highly interested in making cybersecurity changes pushes behaviour across the entire company, but that is the best-case scenario – having a CIO or CISO with pinnacle responsibility over both IT and OT can be enough to push change. Another telling example is given by Hayden: "the CISO is intended to be the security conscience of the company [and] it is their job, or someone equivalent, to get the executives aware and involved." The experts often described personal strengths, such as "telling a good story" (Ryan) or "storytelling" (Steeves), as a key enabler for the security lead in gaining this influence.

In addition to these findings, some respondents gave more detailed suggestions that are worth

including. Both Ryan and Expert 6 expressed how, ideally, the CISO has the respect of, and the ability to influence, the Chief Operations Officer (COO) or the Head of the (Transmission and) Distribution unit. Arguably, there is a built-in contradiction in a CISO originating in the OT sphere, most likely as an engineer or technician, and their effectiveness at influencing the board or C-level colleagues towards prioritising cyber security and incident learning. Most likely the reason is not that the CISO is an outstanding security expert, but because they know the internal dynamics knows how to navigate around the corporate politics. Finding the balance between business acumen and storytelling ability, on the one hand, and sufficient technical skills and security professionalism to ensure their credibility across the organisation, on the other hand, is a formidable human resources challenge.

Moreover, Expert 6 reported advantages for incident learning when firing a CISO following an incident. Sacking the cyber security lead following an incident, such as a data privacy breach, is not uncommon. "Right or wrong is a different question, but it is effective" (Expert 6). The reason for this is that the leadership will wonder what the current CISO has done with the budget allocated to them, whereas a new CISO brings eagerness and fresh energy to the team, which helps set implementation projects in motion.

A point to note is that the dismissal of this executive, raised as an underlying driver for incident learning, is not necessarily a sure-fire way of ensuring success. It takes time for a new cyber security lead to learn about the networks, the architecture, and the people – on both the IT and OT sides. Such risks must be considered.

The process of establishing that the personality and characteristics of the security lead were linked to incident learning, but that it did not match any of the existing indicators, was relatively straightforward as nearly all experts made *verbatim* references to personality and character traits in the individual. A problem arose, however, when deciding whether to create a stand-alone factor, or to include it as a component of senior management commitment. The decision to create a new factor was taken because the definition of senior management commitment chosen for this study puts emphasis on general priority on incident learning by both executives and board members. By contrast, the most important aspect raised by the experts was *the individual characteristics* of the cyber security executive. Steeves put it this way: "You must have the right individual who is leading the charge, who can work the board room and all the way down to the ground level, and make it front of mind."

5.2.2 Incident Impact

The sense of alarm, urgency, and recognition that an incident would have a significant operational and reputational impact upon a DSO make the Incident Impact factor important in principle, experts reported. In real life, the experts generally agree that a lack of real incidents, especially catastrophic ones (e.g., Ukrenergo), undermine the impact of incidents as a driver for incident learning in DSOs. While the experts recognise the perceived seriousness of an incident, whether external or internal, as 'important' or even 'fundamental' for the process of implementing lessons drawn, two problems hamper this factor: the de facto lack of severe incidents and the lack of

transparency in information-sharing, especially regarding OT security incidents between DSOs. "Having a real-world event, not a hypothetical event, is probably the best and easiest way to get the any board member's attention, or CEO's attention" (Ryan). As severe real-world incidents are rare, especially those as sophisticated as the 2016 Ukraine attack, the stimulation of a security culture and the commitment from senior management are interpreted as more important for incident learning than incident impact at this time, as "they will allow a better learning curve" (Rambi). This is evident from the fact that only one expert included Incident Impact among the factors they considered critical for incident learning (Ryan). An interesting perspective is shared by Bodungen: "There is a large portion of the industry that says 'That is the Ukraine, though.' It would be more difficult to achieve that level of outage in the U.S. grid, much more difficult to achieve anything consequential… [CrashOverride] created the opposite reaction in some people in the industry." Yet, Bodungen has also experienced a "direct correlation" between major external incidents and the behaviour of DSOs in terms of attention and spending afforded to cyber security.

Therefore, these findings appear to support the findings by Lampel et al. (2009) and Bartnes et al. (2016) that incident impact is important in principle, but less so in real life under the current circumstances. The expectation for this study, that a minor incident in the IT network that does not affect OT would not lead to more urgency in incident learning whereas an incident affecting OT would, can scarcely be commented upon given the findings. The experts were not able to give detailed-enough examples or simply had not experienced one of the rare serious incidents. While the assumption is logical, the experts perceived the lack of serious incidents as a challenge to incident learning.

5.2.3 Sharing Lessons Drawn

The sharing of lessons drawn was not identified as a key factor for incident learning by experts, although they commonly considered it important in its own right. They rarely tied different methods for Sharing of Lessons Drawn, e.g. informal or formal, to the incident learning process itself. They were rarely associated with the success of an improvement item implementation project. Instead, several common themes emerged.

First, the IT (security) units are perceived not to be open enough to sharing incident lessons internally with other corporate functions for misplaced fear of admitting mistakes. Several experts explained this by referring to how human nature lends us not to share information about things we have been charged with protecting (e.g. Steeves; Tindill). Since the grid is critical, cyber security personnel for IT as well as OT are naturally protective of their area, but this is perceived as "security by obscurity" (Expert 5) by other business lines, which negatively impacts upon the corporate culture. The most noteworthy outcome is perhaps the effect on external lesson-sharing. The perceived lack of transparency in information-sharing between DSOs, especially regarding OT security incidents, is a challenge for the energy utility ISACs (Information Sharing and Analysis Centers) in the U.S. and the recently set-up European counterpart (e.g. Rambi; Tindill; Hayden). If data or intelligence concerning incidents experienced by DSOs are not shared, or shared with insufficient detail, it undermines incident learning through Incident Impact.

Second, the sharing of lessons within the organisation is often determined by, or is subordinate to, other factors, such as structure and culture. Having a preparedness unit ensures that those executives, middle managers, and analysts who need to know about an incident in detail can access that knowledge. By contrast, for incidents like ransomware or data leaks that affect the corporate network, some experts suggested a company-wide message was advisable rather than trusting an informal process, such as "talking about it around the watercooler" (Expert 6). However, the experts' generally struggled to identify lesson-sharing patterns, which appears to suggest that individual DSOs develop them organically. Therefore, it is difficult to claim that this finding discredits the suggestion by Shedden et al. (2010) that informal social networks favoured incident learning by stimulating lesson-sharing across organisations (beyond security). Deeper insight into specific DSOs would be needed to study such networks in detail.

The literature brings up the 'learning agency' that shares lessons drawn internally in the organisation (Argyris and Schön, 1996; Kolb, 1984; Koorneef, 2000). The preparedness unit, and any active case teams, appear to correspond to this idea, albeit in a narrower sense. Whereas the literature suggests an explicit focus on sharing lessons internally, a preparedness unit would help channel them to those concerned as part of an implementation project.

The expectations expressed in Chapter 3 regarding Sharing Lessons Drawn were not fully met. While communication issues between IT and OT units were certainly found to be problematic, these were not tied to the systematic internal sharing of incident lessons as a mechanism for improved incident learning. Instead, the experts appeared to put more faith in external lesson-sharing, especially through ISACs.

5.2.4 Small-Scale Incidents

None of the interviewees found small-scale incidents and near-misses to be critical for incident learning, even though they perceived them as important. They reported that it is considered an industry best practice to use the same post-incident procedure for lesson-drawing and implementation for minor incidents as one would for major incidents. Several equated this to a choice. "Either you pay attention, or you do not" (Rambi). This effectively links the learning from small-scale incidents to security culture and a security mindset that recognises their value. At the same time, the experts identified organisational learning from small-scale incidents as a missed or underutilised opportunity. They generally agreed on the reason as to why this is the case. For an enterprise-siz

ed organisation, small events or incidents happen every day, by the dozens or hundreds depending on one's incident definition. The organisation does not have the luxury of stopping, analysing, debriefing, and creating improvement items to learn – even though it ideally should. They report that so-called blue-sky work, i.e. everyday tasks and responsibilities, occupy one's attention to the detriment of small-scale incidents, accompanied by competing priorities on a management level, including the bottom line (e.g. Steeves; Desautels).

A particular use for small-scale incident learning is, for instance, bad network configuration that are caused by human error, posing a threat to system security (Expert 5). While the impact at a

particular time can be zero, it can be a potential sign of serious weaknesses in network defences. A potential technological solution that was explored with the experts in the interviews was a ticketing system for small-scale incidents that employees across the organisation would use to file cyber security observations or concerns. The experts reported never having observed such systems in use, echoing findings by Bartnes et al (2016), but generally considered this a missed opportunity for incident learning. Theoretically, periodic reviews of such a system can be a preparedness unit's remit.

With regards to the literature, these findings agree that learning from low-impact incidents seems not to be given priority and constitutes an untapped resource (Ahmad et al., 2012; Koornneef, 2000). Contrary to the expectation in Chapter 3, in the experts' experience, DSOs appear not to value small-scale incidents as highly in terms of potential for incident learning as the literature suggests that they should. Small-scale incidents are indeed recognised as important, but it is a factor for incident learning that automatically – or perhaps inherently - follows from the four stand-out factors rather than being prioritised.

5.2.5 Organisational Forgetting

While the experts thought of organisational forgetting as a challenge, none of them considered it a critical factor for incident learning. Rather, they linked it as a sub-theme to the four stand-out factors. For instance, a combination of structure and culture can enable a thorough on-boarding process by long-time staff for new employees often includes modules on business continuity as well as 'after action' processes. Some experts generally linked organisational forgetting to knowledge retention in DSOs more generally rather than linking it specifically to incident learning. (e.g. Steeves; Bodungen).

All experts recognised a potential risk of improvement items 'slipping through the cracks' due to staffing changes, but had not experienced it. Equally, they recognised the problem where staffing changes or retirement can upset the personal trust that underpins the integration of various units in the organisation, not to mention the cyber awareness and psychological safety that drive security culture. Nevertheless, they believed that organisational structures, such as preparedness units, or a strong sense of ownership within the organisation mitigate the risk that organisational realignments will affect implementation projects. The experience of Broekema et al. (2017) that lesson-drawing was affected by organisational forgetting was not explicitly raised, although the author did not systematically probe all experts regarding this. Notably, the above-mentioned practice of firing the CISO to stimulate incident learning is the only instance of unlearning raised (Nystrom & Starbuck, 1984). This makes impossible any further comment on its usefulness, or not, for incident learning.

The expectation in this study that unlearning can be used to jumpstart the incident learning process after major incidents was met, although only a minority of experts had observed this. Organisational forgetting was expected to negatively affect incident learning capability, e.g. if younger, less experiences staff draw the wrong incident lessons, lacking the experience and OT knowledge of retired colleagues. The expectation regarding senior staff having the experience needed to set priorities for learning with regards to planning and preparation, which guides the

implementation (or dismissal) of incident lessons, appears too specific to be addressed given the data collected.

5.2.6 Exercises

The experts emphasised the importance of regular exercises. Yet, only a couple of the experts perceived exercises as one of their *most critical* factors for successful incident learning. A common reason given by the experts for this is that the practical usefulness of lessons drawn from exercises are contingent upon organisational culture and senior management commitment (e.g. Ryan, Rambi). All experts believed that the same evaluation and improvement item implementation process should be used whether an incident is real or an exercise. They also agreed that DSOs should spend more resources on more frequent exercises. There was general agreement that, if exercise scenarios draw on actual incidents or otherwise guarantee high levels of realism and chaos, exercising can be of similar effectiveness as actual incidents, up to a certain point where the critical mass of a real incident will lend additional urgency that drives incident learning. For example, Steeves stated that "we try to make the exercises as chaotic, unfamiliar and realistic as if they were woken up at 2 am and had to come into work." Desautels exemplified further: "if they are all over the newspapers, or have regulators coming in, that has a different impact real-world to exercises - but on a general day, they are equally as effective." Notably, Expert 6 raised red team exercises as particularly helpful for incident learning in that the simulation of a committed adversary provides additional realism.

The literature raised the issue of blame games as a factor that would impede organisational learning from exercises. It also raised the usefulness of exercises for diffusing tension or 'blame culture' within an organisation (Donahue & Tuohy, 2006; Trim & Upton, 2013). Only a few experts brought this up as a reason why exercises are important for incident learning. For instance, Bodungen holds that "this is where exercises work better than real-life incidents because in a real-life incident you may not have the ability to replay the incident and show a chain of events that happened." While the experts gave a sense of low priority for exercises (e.g. Rambi, Steeves), the findings do not link to the lack of major incidents, as found by Bartnes et al. (2016). However, given the exploratory interview guide, the author did not specifically ask about such a link.

Contrary to the expectation for this study, the experts did not reference a sense of urgency in DSOs arising from a realisation after conducting cyber security exercises that their incident readiness was worse than anticipated – in contrast to Bartnes et al. (2016). Since this study was exploratory in nature and did not seek to investigate causal relationships at a deeper level, it is difficult to comment further.

The findings can be interpreted to mean that, just like lessons from actual incidents, lessons from exercises will be much more likely to be implemented promptly if the organisational culture is already conducive to incident learning. It is preferrable if the structure is such that the preparedness unit dedicated to tracking improvement items (ownership, completion, timeline) can pick up on lessons from exercises using the same procedure as for real incidents. Exercises in themselves are not a critical factor but exercises are part of a security-committed and security-conscious organisation that is structured to learn from (simulated) incidents.

6 CONCLUSION

While the concept of organisational learning has received widespread attention from academics for decades, less attention has been paid to organisational learning from incidents, especially in the cyber security domain where the technology perspective still dominates. Similarly, while emergency management in electric utilities has been a key practitioner concern for decades, the incident management process has received little academic attention, especially regarding cyber security. This thesis has addressed this state of affairs by exploring what factors in an electric distribution company drive cyber incident learning. Cyber incident learning was operationalised as successful implementation of lessons drawn from incidents. Empirical data on the incident learning process was collected by interviewing key experts with insight into industrial control systems and cyber security in electric utilities. In conclusion, the factors found to be most important in a successful incident learning capability were organisational structure, organisational culture, senior management commitment, and regulatory pressure. Between these, organisational culture – the building of a security culture based on risk management, cyber awareness, and trust – was the most important, as perceived by the experts. As secondary or underpinning factors, the individual traits of the cyber security lead, incident impact, internal sharing of lessons, small-scale incidents, (mitigation of) organisational forgetting, and exercises were found to be less important. More broadly, it can be concluded that incident learning is a complex process. The various factors that drive it are often simultaneous and intersecting. This creates difficulty in determining which are most important.

Since electric distribution companies typically have highly limited resources, owing in part to their unfavourable position in the smart grid transformation, the identification in this study of four key factors for incident learning is believed to be useful scholars and academics alike. While all factors under study seem intertwined in the incident learning process, none appear more so than organisational structure, security culture, and senior management commitment. Therefore, the concept of an incident learning triad is suggested as a key driver of an effective incident learning capability in DSOs. As for the fourth key factor, the prominence of regulatory pressure for driving incident learning in the experts' views was unexpected as the literature had not stressed this relationship. The effects of the four key factors upon each other and their respective causal links to the incident learning process cannot be inferred further given the limited data sources and limited organisational access inherent in this exploratory research design. Nonetheless, the indication that the four factors are crucially important lines up with extant literature and highlights an incentive for further research into them. This indication is believed to be useful for executives as well as emergency and incident managers in DSOs.

6.1 THEORETICAL IMPLICATIONS

Overall, the body of knowledge used as reference points when building indicators in this study proved appropriate for the responses from interviewees to the exploratory and explanatory questions posed to them. This can be seen in the fact that all factors for incident were referred to as relevant. Neither the electric distribution utility industry nor the field of cyber security incidents appear to call for radically different theoretical concepts for incident learning.

With regard to findings by others that incident learning is difficult and often narrowly focussed on incident response (Bartnes et al., 2016; Grispos et al., 2017; Jaatun et al., 2009; Shedden et al., 2010), two conclusions can be drawn. First, this study is outcome-driven by design, exploring critical success factors as perceived by key experts rather than 'measuring' incident learning. Therefore, the relative difficulty of the incident learning process cannot be commented upon, but it can be concluded through the experts' interviews and experiences that incident learning does occur. Second, the scope in this study was focussed on the incident learning process more broadly. The findings can be linked to pro-active incident learning, i.e. when the "incident handling system is adjusted based on lessons learned internally and in the context of the organization" (Jaatun et al., 2009, p. 35; Line et al., 2008). This is because the theory-derived factors found by this study to be linked to incident learning are instructive for building such a pro-active incident learning capability. Similarly, there are implications for double-loop theory (Argyris & Schön, 1978). A DSO that seeks to build an incident learning capability that goes beyond incident response itself could use the findings in this study as indications of the factors that will enable it to engage in double-loop learning. That is, the factors can help the organisation "reconsider and alter their fundamental rules, policies, systems and processes in order to promote longterm change" (Shedden et al., 2010).

AVENUES FOR FURTHER RESEARCH

As for avenues for further research, the first recommendation is a robust quantitative survey-based study seeking to verify (or not) the relative importance of the various factors for incident learning found to be key or supporting, respectively, in this study. The indication that the triad for incident learning, namely structure, culture, and senior management commitment, is particularly important for incident learning merits attention. The theoretical link between leadership and culture (Flores et al., 2012; Trim & Upton, 2013) is supported by this study, as is the link between organisational structure and culture (Meyer, 1982). Further study of the literature could probably strengthen this relationship in general, while theory-testing of this link in an industrial context – as well as in a general cyber incident learning context – could generate evidence of more solid causal theories on how organisations may design their incident learning capabilities.

The second specific recommendation is to conduct a deeper study into the different facets of organisational culture in DSOs, focussing on how the organisational context interacts with cyber security incidents and the influence of this on incident learning. For instance, the importance of a risk management mindset as part of culture was not suggested by the literature review in this study. More broadly, a more rigorous study into the effect of various cultural sub-factors (e.g., Flores et al., 2012) could help pinpoint the mechanisms that lead to a successful incident learning process in industrial cyber security contexts.

The third specific recommendation regards the two new factors, regulatory pressure and individual traits in the cyber security lead. They were created as they could not be coded to existing indicators. Both merit further literary research and theory-testing with respect to the management literature to scrutinise their role in driving incident learning in the electric utility industry. In particular, the indication that personal characteristics, such as story-telling ability and respectability, help build security culture and help convince executives to spend resources on cyber security merits more

focussed research. It could result in more substantiated theories regarding the role of individuals in incident learning.

LIMITATIONS

The chief limitation in this thesis is the reliance on key experts' perceptions and experiences for data collection, which negatively influences confirmability. If the study were repeated with other with different backgrounds, the findings may shift. The variety of backgrounds used in this study may also provide a more general but also more representative view of the general incident learning process in DSOs. This limits the level of detail in the research regarding potential causal links and drivers of incident learning, which explains the relatively modest conclusions drawn above.

The author experienced an unwillingness to talk about cyber security in general, and incidents and learning in particular, among DSOs, echoing Jaatun et al. (2009). Consequently, the reliance on a single data source is a weakness of this study. Moreover, the lack of previous documented studies (that the author was able to find) proved a methodological challenge since little information was available to allow desktop research as an additional data source. This also helped shape the study into an exploratory study. On the other hand, the mixed positions among the experts, both consultants and employees of DSOs, helps provide wider perspectives and a more holistic inquiry into incident learning. Given the scope of the study as an exploratory study, aimed at giving an initial indication of incident learning factors in DSOs, it was felt that these weaknesses would be acceptable.

Another issue regarding confirmability is that this exploratory study did not use an irrefutable tool for judging the relative importance of the respective incident learning factors. However, there will always be an element of interpretation. Credibility is supported by the fact that open questions were asked in the beginning of the interviews to avoid leading the key experts to favour certain views. Upon reviewing a draft of the findings, the experts found the findings reasonable with reference to their interview experiences and all agreed to have their names published (except those who could not for other reasons).

The transferability of this study and its findings onto other contexts or settings is limited. There are somewhat similar organisational divides in terms of, for example, structure and culture in other industries, such as oil and gas, that operate industrial control systems and face rises in cyber security threats. The security mindset, especially the role of risk management, can help them realise that cyber security and incidents have a direct impact upon them. More open and transparent external lesson-sharing will also likely be applicable. However, factors such as market conditions and other operating conditions between DSOs and ICS-operating utilities in general can differ significantly, wherefore the responsibility rests with each interested party to investigate whether the enabling factors found to be important in this study can inform the incident learning process in their organisation.

6.2 PRACTICAL RECOMMENDATIONS

The findings of this exploratory study can serve as a baseline for managers and executives of electric utilities, as well as utility consultants. The following indications related to successful incident learning are opportunities for DSOs to compare their current practices and priorities to the perceptions of industry experts:

- The creation of a security culture seems to favour incident learning. This includes the realisation by all corporate functions that cyber threats to the corporate network as well as control systems have a direct impact upon them. To build security culture, it should be made a strategic objective of the organisation to ensure executive commitment and sufficient resources. Also, enterprise-wide training to build awareness of cyber threats and confidence to report anomalies are components of security culture.
- A risk management mindset can be extended to include cyber security as part of security culture. This helps prioritise the most impactful instances of incident learning and helps ensure that this process is a priority for executives and board members.
- Trust between IT and OT personnel can favour incident learning. The stimulation of personal ties between these groups is tool to this end, for example as part of remediations projects in cyber security. Note that outsourcing can be disadvantageous in this regard since it typically decreases personal connections.
- The hiring of CISO with a strong character and story-telling ability is linked to successful incident learning. The ability to influence C-level colleagues and board members of the need to spend resources on incident learning is important for incident learning.
- Exercises are important for incident learning, not to mention incident response capability. The more realistic they are, the better. Consider, for example, red team engagements.
- A dedicated preparedness unit seems to favour incident learning. By formalising the post-incident learning process, such a unit drives incident learning by ensuring accountability for the on-schedule implementation of lessons drawn. It also helps integrate different business units, again stimulating cross-unit personal relationships.
- IT/Cyber security leaders may want to pro-actively run shared projects between IT and other units – including OT, but also beyond - if the structure of the organisation is going to stimulate both cyber security posture and incident learning. This lets them interface with other lines of business and draw attention to their work.

Concluding Remark

This thesis has made a small attempt to counter the tide of technology-heavy research into cyber security through its focus on people and process in securing not only information and operations, but the greater security of today's electricity-dependent societies.

7 BIBLIOGRAPHY

Accenture. (2017). *Outsmarting Grid Security Threats POV | Accenture*. Retrieved from https://www.accenture.com/t20170928T152847Z__w__/us-en/_acnmedia/PDF-62/Accenture-Outsmarting-Grid-Security-Threats-POV.pdf#zoom=50

Accenture. (2018). *Threatscape Report 2018*.

Accenture Strategy. (2016). *Electricity Network Transformation Roadmap: Insights from Global Jurisdictions, New Market Actors & Evolving Business Models*. Retrieved from https://www.accenture.com/t00010101T000000Z__w__/au-en/_acnmedia/PDF-49/Accenture-Energy-Networks-Australia-CSIRO-Roadmap-Summary-Report.pdf

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams – Challenges in supporting the organisational security function. *Computers & Security*, *31*(5), 643–652. https://doi.org/10.1016/j.cose.2012.04.001

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management*, *35*(6), 717–723. https://doi.org/10.1016/j.ijinfomgt.2015.08.001

Argote, L. (2012). *Organizational Learning: Creating, Retaining and Transferring Knowledge*. Springer US. Retrieved from https://books.google.nl/books?id=sNpKMgEACAAJ

Argyris, C., & Schön, D. A. (1978). *Organizational learning: a theory of action perspective*. Addison-Wesley Pub. Co. Retrieved from https://books.google.nl/books?id=2aYOAQAAMAAJ

Argyris, C., & Schön, D. A. (1996). *Organizational Learning II: Theory, Method, and Practice*. Addison-Wesley Publishing Company. Retrieved from https://books.google.nl/books?id=3aMoAQAAMAAJ

Ashford, W. (2018, February 28). Firms failing to learn from cyber attacks. *ComputerWeekly.Com*. Retrieved from https://www.computerweekly.com/news/252435869/Firms-failing-to-learn-from-cyber-attacks

Bartnes, M., Moe, N. B., & Heegaard, P. E. (2016). The future of information security incident management training: A case study of electrical power companies. *Computers and Security*, *61*, 32–45. https://doi.org/10.1016/j.cose.2016.05.004

Bourque, L. B. (2004). Cross-Sectional Design. In M. S. Lewis-Beck, A. Bryman, & T. Futing Liao (Eds.), *The SAGE Encyclopedia of Social Science Research Methods*. Thousand Oaks, CA: SAGE Publications, Inc. https://doi.org/http://dx.doi.org/10.4135/9781412950589.n204

Bowditch, J. L., Buono, A. F., & Stewart, M. M. (2007). *A Primer on Organizational Behavior*. Wiley. Retrieved from https://books.google.nl/books?id=Mu9wDwAAQBAJ

Broekema, W., van Kleef, D., & Steen, T. (2017). What Factors Drive Organizational Learning From Crisis? Insights From the Dutch Food Safety Services' Response to Four Veterinary Crises. *Journal of Contingencies and Crisis Management*, *25*(4), 326–340. https://doi.org/10.1111/1468-5973.12161

Byres, E. (2013). The air gap: SCADA's enduring security myth. *Communications of the ACM*, *56*(8), 29. https://doi.org/10.1145/2492007.2492018

Catino, M. (2008). A Review of Literature: Individual Blame vs. Organizational Function Logics in Accident Analysis. *Journal of Contingencies and Crisis Management*, *16*(1), 53–62. https://doi.org/10.1111/j.1468-5973.2008.00533.x

Catino, M., & Patriotta, G. (2013). Learning from Errors: Cognition, Emotions and Safety Culture in the Italian Air Force. *Organization Studies*, *34*(4), 437–467. https://doi.org/10.1177/0170840612467156

Cherepanov, A. (2017). WIN32/INDUSTROYER: A new threat for industrial control systems. ESET.

Child, J. (1984). *Organization — A Guide to Problems and Practice* (2nd Ed). New York: Harper & Row. https://doi.org/10.1177/017084068500600318

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. *NIST Special Publication*, *800–61*, 79. https://doi.org/10.6028/NIST.SP.800-61r2

Connell, L. J. (2004). Linking Risk Assessment and Risk Management. In J. R. Phimister, V. M. Bier, & H. C. Kunreuther (Eds.), *Accident Precursor Analysis and Management: Reducing Technological Risk Through Diligence*. Washington, DC: The National Academies Press. https://doi.org/10.17226/11061

Crossan, M., Lane, H., & White, R. E. (1999). An Organizational Learning Framework : From Intuition to Institution. *Academy of Management Proceedings*, *24*(3), 522–537. https://doi.org/10.2307/259140

Dekker, S. W. A. (2009). Just culture: who gets to draw the line? *Cognition, Technology & Work*, *11*(3), 177–185. https://doi.org/10.1007/s10111-008-0110-7

Denzin, N. K., & Lincoln, Y. S. (1994). *Handbook of Qualitative Research* (2nd ed.). Thousand Oaks, CA: SAGE Publications, Inc.

Donahue, A. K., & Tuohy, R. V. (2006). Lessons We Don't Learn : A Study of the Lessons of Disasters , Why We Repeat Them, and How We Can Learn Them. *Homeland Security Affairs*, *II*(2), 1–28. https://doi.org/10.2310/8000.2011.110386

Dragos Inc. (2017). CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations, 1–35.

Drupsteen, L., & Guldenmund, F. W. (2014). What Is Learning? A Review of the Safety Literature to Define Learning from Incidents, Accidents and Disasters. *Journal of Contingencies and Crisis Management*, *22*(2), 81–96. https://doi.org/10.1111/1468-5973.12039

Duncan, R. B. (1974). Modifications in decision structures in adapting to the environment: Some implications for organizational learning. *Decision Sciences*, 705–725.

Edmondson, A. (1999). Psychological Safety and Learning Behavior in Work Teams. *Administrative Science Quarterly*, *44*(2), 350–383.

Fiol, C. M., & Lyles, M. A. (1985). Organizational learning. *The Academy of Management Review*, *10*(4), 803–813.

Flamholtz, E., & Randle, Y. (2014). Implications of organizational Life Cycles for Corporate Culture and Climate. In K. M. Barbera & B. Schneider (Eds.), *The Oxford Handbook of Organizational Climate and Culture*. Oxford: Oxford University Press.

Flores, L. G., Zheng, W., Rau, D., & Thomas, C. H. (2012). Organizational Learning: Subprocess Identification, Construct Validation, and an Empirical Test of Cultural Antecedents. *Journal of Management*, *38*(2), 640–667. https://doi.org/10.1177/0149206310384631

Gartner. (n.d.). Operational Technology (OT). Retrieved January 8, 2019, from

https://www.gartner.com/it-glossary/operational-technology-ot/

Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., & Good, T. (2006). *SP 800-84. Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*. Gaithersburg, MD, United States: National Institute of Standards & Technology.

Greenberg, A. (2017). Crash Override: The Malware That Took Down a Power Grid. *Wired*, 1–13.

Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*, 1–22.

Greenberg, J. (2011). *Behavior in organizations* (10th ed.). Upper Saddle River, NJ.

Grispos, G., Glisson, W. B., & Storer, T. (2017). Enhancing security incident response follow-up efforts with lightweight agile retrospectives. *Digital Investigation*, *22*, 62–73. https://doi.org/10.1016/j.diin.2017.07.006

Guri, M., & Elovici, Y. (2018). Bridgeware: The Air-gap Malware. *Communications of the ACM*, *61*(4), 74–82. https://doi.org/10.1145/3177230

Haddon, A. (2012). Outcome-Driven Research. In A. J. Mills, G. Durepos, & E. Wiebe (Eds.), *Encyclopedia of Case Study Research* (pp. 640–641). Thousand Oaks, CA: SAGE Publications, Inc. https://doi.org/10.4135/9781412957397

Hay Newman, L. (2018, November 28). Russian hackers haven't stopped probing the US power grid. *Wired*, pp. 1–9. Retrieved from https://www.wired.com/story/russian-hackers-us-power-grid-attacks/

Hollnagel, E. (2011). *Resilience Engineering in Practice: A Guidebook*. Ashgate. Retrieved from https://books.google.nl/books?id=L9qTAQAACAAJ

Homsma, G. J., Van Dyck, C., De Gilder, D., Koopman, P. L., & Elfring, T. (2009). Learning from error: The influence of error incident characteristics. *Journal of Business Research*, *62*(1), 115–122. https://doi.org/10.1016/j.jbusres.2007.12.003

Hovden, J., Størseth, F., & Tinmannsvik, R. K. (2011). Multilevel learning from accidents – Case studies in transport. *Safety Science*, *49*(1), 98–105. https://doi.org/10.1016/j.ssci.2010.02.023

Hsieh, H.-F., & Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Health Research*, *15*(9), 1277–1288. https://doi.org/10.1177/1049732305276687

IER. (2014). Grid Schematic. Institute for Energy Research. Retrieved from https://www.instituteforenergyresearch.org/wp-content/uploads/2014/09/schematic.png

ISO/IEC. (2016). ISO/IEC 27035:2016 Information technology - Security techniques - Information security incident management. Geneva, Switzerland: International Organization for Standards.

Jaatun, M. G., Albrechtsen, E., Line, M. B., Tøndel, I. A., & Longva, O. H. (2009). A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*, *2*(1–2), 26–37. https://doi.org/10.1016/j.ijcip.2009.02.004

Jaques, T. (2007). Issue management and crisis management: An integrated, non-linear, relational construct. *Public Relations Review*, *33*(2), 147–157. https://doi.org/10.1016/j.pubrev.2007.02.001

Kargl, F., Van Der Heijden, R. W., König, H., Valdes, A., & Dacier, M. C. (2014). Insights on the

security and dependability of industrial control systems. *IEEE Security and Privacy*, *12*(6), 75–78. https://doi.org/10.1109/MSP.2014.120

King, N. (2004). Using Interviews in Qualitative Research. In C. Cassell & G. Symon (Eds.), *Essential Guide to Qualitative Methods in Organizational Research*. London: SAGE Publications Ltd. https://doi.org/10.4135/9781446280119

Kletz, T. A. (2008). Searchlights from the past. *Journal of Hazardous Materials*, *159*(1), 130–134. https://doi.org/10.1016/j.jhazmat.2007.09.119

Kolb, D. A. (1984). (1984). *Experiential Learning*. Englewood Cliffs, NJ: Prentice Hall.

Koornneef, F. (2000). *Organised Learning from Small-scale Incidents*. TU Delft.

Kott, A., & Linkov, I. (2019). *Cyber Resilience of Systems and Networks*. (A. Kott & I. Linkov, Eds.) (eBook). Springer International Publishing. https://doi.org/10.1007/978-3-319-77492-3

Kral, P. (2011). *Incident Handler's Handbook*. SANS Institute.

Kumar, R. (2010). *Research Methodology: A Step-by-Step Guide for Beginners*. SAGE Publications.

Kvale, S., & Brinkmann, S. (2009). *InterViews: Learning the Craft of Qualitative Research Interviewing*. SAGE Publications. Retrieved from https://books.google.nl/books?id=bZGvwsP1BRwC

Lampel, J., Shamsie, J., & Shapira, Z. (2009). Experiencing the Improbable: Rare Events and Organizational Learning. *Organization Science*, *20*(5), 835–845. https://doi.org/10.1287/orsc.1090.0479

Leavitt, H. (1964). Applied organization change in industry : structural, technical, and human approaches. In W. W. Cooper (Ed.), *New perspectives in organization research*. New York: Wiley.

Line, M. B., & Albrechtsen, E. (2016). Examining the suitability of industrial safety management approaches for information security incident management. *Information & Computer Security*, *24*(1), 20–37. https://doi.org/https://doi.org/10.1108/ICS-01-2015-0003

Line, M. B., Albrechtsen, E., & Jaatun, M. G. (2008). A Structured Approach to Incident Response Management in the Oil and Gas Industry. In *Critical Information Infrastructure Security, Third International Workshop, CRITIS 2008, Rome, Italy, October 13-15, 2008*. (Vol. 5508, pp. 235–246). https://doi.org/10.1007/978-3-642-03552-4_21

Lukic, D., Littlejohn, A., & Margaryan, A. (2012). A framework for learning from incidents in the workplace. *Safety Science*, *50*(4), 950–957. https://doi.org/10.1016/j.ssci.2011.12.032

Maj, M., Reijers, R., & Stikvoort, D. (2010). *Good Practice Guide for Incident Management*. Heraklion, Greece: ENISA.

Meyer, A. D. (1982). Adapting to Environmental Jolts. *Administrative Science Quarterly*, *27*(4), 515–537.

Muhren, W. J., Eede, G. Van Den, & de Walle, B. Van. (2007). Organizational Learning for the Incident Management Process: Lessons from High Reliability Organizations. In H. Österle, J. Schelp, & R. Winter (Eds.), *Proceedings of the Fifteenth European Conference on Information Systems, {ECIS} 2007, St. Gallen, Switzerland, 2007* (pp. 576–587). University of St. Gallen. Retrieved from http://aisel.aisnet.org/ecis2007/65

National Coordinator for Security and Counterterrorism of the Netherlands. (2018). Cyber Security Assessment of the Netherlands, 76.

Nystrom, P. C., & Starbuck, W. H. (1984). To Avoid Organizational Crises, Unlearn.

Organizational Dynamics, *Spring*, 53–75.

O'Reilly, C. A., & Chatman, J. A. (1996). Culture as social control: Corporations, cults, and commitment. In B. M. Staw & L. Cummings (Eds.), *Research in Organizational Behavior* (pp. 157–200). Stamford, CT: JAI Press.

Penuel, K., Statler, M., & Hagen, R. (2013). *Encyclopedia of Crisis Management*. Thousand Oaks, CA: SAGE Publications, Inc. https://doi.org/10.4135/9781452275956

Pfeffer, J. (1991). Organization Theory and Structural Perspectives on Management. *Journal of Management*, *17*(4), 789–803. https://doi.org/10.1177/014920639101700411

Robbins, S. P. (1990). *Organization theory : structure, design, and applications* (3rd Ed.). Englewood Cliffs, N.J.: Prentice Hall.

Sabatier, P. A. (1987). Knowledge, Policy-Oriented Learning, and Policy Change. *Knowledge: Creation, Diffusion, Utilization*, *8*(4), 649–692.

Schöbel, M., & Manzey, D. (2011). Subjective theories of organizing and learning from events. *Safety Science*, *49*(1), 47–54. https://doi.org/10.1016/j.ssci.2010.03.004

Scholl, F., & Mangold, M. (2011). Proactive incident response. *The Information Systems Security Association Journal*, *9*(2).

Scholten, L. (2018). Tientallen ondernemingen getroffen: Nieuwe gijzelsoftware treft ook Nederland. Retrieved from https://www.fox-it.com/nl/insights/blogs/blog/nieuwe-gijzelsoftware-treft-ook-nederland/

Schwab, A. (2007). Incremental Organizational Learning from Multilevel Information Sources: Evidence for Cross-Level Interactions. *Organization Science*, *18*(2), 233–251. https://doi.org/10.1287/orsc.1060.0238

Shedden, P., Ahmad, A., & Ruighaver, A. B. (2010). Organisational learning and incident response: Promoting effective learning through the incident response process. *Proceedings of the 8th Australian Information Security Management Conference*, (November). https://doi.org/10.4225/75/57b6771734788

Shedden, P., Scheepers, R., Smith, W., & Ahmad, A. (2011). Incorporating a knowledge perspective into security risk assessments. *VINE*, *41*(2), 152–166. https://doi.org/10.1108/03055721111134790

Shrivastava, P. (1983). A Typology of Organizational Learn. *Journal of Management Studies*, *20*(1), 7–28. https://doi.org/10.1111/j.1467-6486.1983.tb00195.x

Smith, D., & Elliott, D. (2007). Exploring the barriers to learning from crisis: Organizational learning and crisis. *Management Learning*, *38*(5), 519–538. https://doi.org/10.1177/1350507607083205

Stebbins, R. A. (2008). Exploratory Research. In L. M. Given (Ed.), *The Sage Encyclopedia of Qualitative Research Methods* (pp. 327–329). Thousand Oaks, CA: SAGE Publications Ltd. https://doi.org/10.1007/s00044-009-9284-7

Streb, C. K. (2012). Exploratory Case Study. In A. J. Mills, G. Durepos, & E. Wiebe (Eds.), *Encyclopedia of Case Study Research* (pp. 372–373). Thousand Oaks: SAGE Publications, Inc. https://doi.org/10.4135/9781412957397.n139

Symantec Corporation. (2014). *Dragonfly: Cyberespionage Attacks Against Energy Suppliers*.

Symantec Corporation. (2018). SamSam : Targeted Ransomware Attacks Continue. Retrieved December 6, 2018, from https://www.symantec.com/blogs/threat-intelligence/samsam-targeted-ransomware-attacks

Thomas, D. R. (2006). A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation*, *27*(2), 237–246. https://doi.org/10.1177/1098214005283748

Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers and Security*, *45*, 42–57. https://doi.org/10.1016/j.cose.2014.05.003

Trim, P. R. J., & Upton, D. (2013). *Cyber Security Culture: Counteracting Cyber Threats Through Organizational Learning and Training*. Gower. Retrieved from https://books.google.se/books?id=mredMQEACAAJ

Trochim, W., & Donnelly, J. P. (2006). *The Research Methods Knowledge Base*. Cengage Learning. Retrieved from https://archive.org/details/WilliamTrochimJamesPDonnellyTheResearchMethodsKnowledgeBase2006/page/n161

van Duin, M. J. (1992). *Van Rampen Leren*. Leiden.

8 APPENDIX A – INTERVIEW GUIDE

The guide is written with flexibility in mind such that it can be used both for interviewees who are employees of electric utilities and consultants for such companies. Each interview started with repeating a summary of the research objective and the definition of incident learning used in this study, even though this information was always included in the first email exchange that preceded the interview.

8.1 INITIAL CONVERSATION

This conversation was, as explained in the Interview Guide (Section 4.2.1), always carried out but not recorded due to the potentially sensitive nature of the information elicited.

1. What are your organisation's core business areas in 2 sentences?
2. What is your role within the organisation?
3. Are you involved in post-incident activity in-house, with clients, or both?
4. Is your organisation using a standard methodology or guideline for cyber security incident response, like NIST, SANS, ISO/IEC or ENISA?
5. How is IR structured in your organisation? Separate team/function? Outsourced in case of CSIRT?)
    a. Does your organisation use similar procedures for lesson-drawing from cyber incidents as for physical disruptions?
6. How should a successful post-incident investigation into lesson-to-be-learned be done, in your experience?
    b. When is this done?
    c. How is this done?
    d. Who participates?

8.2 GENERAL QUESTIONS

A variant of the research question is asked in an open manner to elicit the expert's spontaneous answers as to what factors or conditions are important for the incident learning process to be successful. Follow-up questions were asked as appropriate.

1. In your experience from DSOs, what are the enablers for successful implementation of lessons drawn after a cyber incident?
2. From a general perspective, what conditions or factors have you found to be critical in ensuring that lessons drawn from cyber security incidents get implemented and result in organizational change?
3. What features stood out to you in DSOs where you have observed effective continuous learning processes?

8.3 FACTOR-SPECIFIC

This part focusses on the respective factors for incident learning derived from the literature. It consists of an overarching pair of questions for each factor and several supporting questions that can be used to probe the interviewee on underlying causes as to why a factor might be important for incident learning (or not). Due to time constraints and the exploratory objective, the interviews did not cover all supporting questions.

8.3.1 Organisational Structure

Main questions:

- Is organisational structure important in explaining if lessons drawn from cyber incidents get implemented or not in your organisation/in DSOs you have insight into? Why/why not?
- How does the structure of your organisation influence the process of learning from previous incidents?

Possible probing questions:

1. How does the cyber IR team (depending on Intro question 5) interact with other company departments in the post-incident phase?
2. Where should the authority to make decisions be concentrated to ensure that an LD is implemented?
3. Who should have the most power to make decisions to ensure that an LD is implemented?

8.3.2 Organisational Culture

Main question:

- Is organisational culture important in explaining if lessons drawn from cyber incidents get implemented or not in your organisation? Why/why not?
- What is the role culture of your organisation in driving the (successful) process of drawing lessons from previous incidents and implementing those?

Possible probing questions:

1. What effects does the cyber-physical (IT/OT/physical equipment) nature of the organisation have on the incident learning process?
2. In your experience, what values (interpersonal, job importance) do organisations that are successful in learning from past incidents promote? How do they promote them?
3. How do mutual understanding, communication and collaboration between IT staff and control system (OT) staff affect the implementation of incident lessons?
4. Are employees encouraged or rewarded for reporting or discussing incident information?

8.3.3 Incident Impact

Main questions:

- Is the perceived impact of an incident (severity) important in explaining if lessons drawn from cyber incidents get implemented or not in your organisation? Why/why not?
- How does the perceived seriousness of the incident influence the process of implementing lessons drawn in your organisation?

Possible probing questions:

1. Is it necessary that all/the majority of staff believe the incident to be severe for OL to take place, or is it enough if a few key players believe it is severe? Who?
2. How does the passage of time affect the implementation of new ideas and improvements following an incident?
3. How does your organisation learn from small-scale incidents or near misses?

8.3.4 Senior Management Commitment

Main questions:

- Is a commitment to OL among senior management important in explaining if lessons drawn from cyber incidents get implemented or not in your organisation? Why/why not?
- How does senior management commitment in your organisation influence the process of learning from previous incidents?

Possible probing questions:

1. Are senior managers active in creating a culture that embraces change/adaptation?
2. What is the most important instrument that top managers have for ensuring IL?
3. Do senior managers involve employees who were directly affected by an incident in the post-incident phase?
4. Are employees from across the whole organisation involved in the IL process? Why/not?

8.3.5 Sharing Lessons Drawn

Main questions:

- Is the sharing of incident lessons important in explaining if they get implemented or not in your organisation? Why/why not?
- How does the sharing of lessons drawn from previous incidents organisation influence the process of learning from them?

Possible probing questions:

1. What are effective sharing methods internally that lead to IL, if any?
2. Is the sharing formal? How informal is it?
3. Who is in charge of sharing lessons from past incidents?
4. Are lessons shared externally?

8.3.6 Small-Scale Incidents

Main questions:

- Does your organisation pay attention to small-scale incidents and near misses and draw lessons from them for future preparation and IR? Why/why not?
- How are small-scale incidents used in the IL process?

Possible probing questions:

1. Can small-scale incidents be useful for developing incident preparation and response given that there are so few major incidents?
2. Is there a ticketing system for follow-up, or should there be?
3. Is there a focus on 'high impact' incidents in your organisation? Is this negative?

8.3.7 Organisational Forgetting

Main questions:

- Is organisational forgetting a factor in explaining if lessons drawn from cyber incidents get implemented or not in your organisation? How does organisational forgetting in your organisation influence the process of learning from previous incidents?

Possible probing questions:

1. How does a loss of experience (e.g. retirement, relocation) affect the planning and preparation for future incidents?
2. Is the systems knowledge of older staff who retire valuable given increased IT integration?
3. Would 'unlearning' by changing (all) top managers of your organisation help its IL process?

8.3.8 Exercises and Simulations

Main questions:

- Are incident simulation exercises a factor in explaining if lessons drawn from cyber incidents get implemented or not in your organisation? Why/why not?
- How do exercises and simulations of incidents influence the process of learning from previous incidents?

Possible probing questions:

1. Should there be more funding for exercises?
2. Do exercises take too much time from 'real work'?
3. How do exercises change the feeling of readiness for an incident, if at all?

[End of Interview]