NTNU – Trondheim
Norwegian University of
Science and Technology

Outsourced incident management services

Alfredo Ramiro Reyes Zuniga

Master in Security and Mobile Computing
Submission date: June 2015
Supervisor: Colin Alexander Boyd, ITEM
Co-supervisor: Martin G Jaatun, SINTEF
Tuomas Aura, Aalto University

Norwegian University of Science and Technology
Department of Telematics

Title: Outsourced incident management services

Student: Alfredo Ramiro Reyes Zúñiga

Problem description:

Outsourcing incident management services seems to be a cost-effective way to satisfy some small and large organization's security requirements. This topic is currently not well-explored by researchers, hence further investigations are needed to identify whether there are specific challenges of relying on outsourced services for incident management, such as prevention, detection and response. How do outsourced incident management services benefit or affect current incident management teams?

This project will address the following research questions:

- How are roles, responsibilities and penalties described in service level agreements between a customer and the outsourced incident management service's provider?
- Which challenges are experienced during the implementation of these services throughout the incident response life-cycle?
- What are the future needs for outsourced incident management and what is lacking from the industry to make it real?

The project will be carried out as a case study based on interviews and document analysis supported by literature review on related work.

Responsible professor: Colin Boyd, ITEM

Supervisor: Martin G. Jaatun, SINTEF

Abstract

With increasing use of information and communication technologies (ICT), many organizations are outsourcing information security services to managed security service providers (MSSP). This project reports results on current practice and experiences with outsourced incident management services. The research was conducted as a case study performing a qualitative study of six large MSSPs, one emerging MSSP and an independent expert. The findings reveal multiple challenges that both customers and providers are currently facing, including suggestions for addressing them. This information will be useful for organisations looking to improve their practices. This research seeks to build awareness of the challenges posed by relying on outsourced services for incident management. It describes how these services are benefiting or affecting current incident management teams and some of the future needs of this field. Furthermore, it contributes with a categorization of the services offered by some of the most significant MSSPs in the market.

Acknowledgements

I would like to acknowledge the effort invested by everyone who participated in the interviews that this thesis is based on. Without their cooperation the thesis would not have been feasible.

I would also like to give a heartfelt thank you to Martin G. Jaatun, Colin A. Boyd and Tuomas Aura. All of them encouraged my undertaking a thesis that was in line with my engagement as information security professional and my research interests.

I also want to warmly thank my family for all the moral support, patience, encouragement and the amazing chances they have given me over the years.

Contents

List of Figures

List of Tables

List of Acronyms

BPO Business Process Outsourcing

CERT Computer Emergency Response Team

CERT-CC Computer Emergency Response Team - Coordination Center

CIO Chief Information Officer

CIRT Computer Incident Response Team

CISO Chief Information Security Officer

CSIRT Computer Security Incident Response Team

CybOX Cyber Observable Expression

ENISA European Network and Information Security Agency

DDoS Distributed Denial of Service

DLP Data Loss Prevention

DoS Denial of Service

ICT Information and Communication Technology

IEC International Electro-technical Commission

IOC Indicators of Compromise

IRT Incident Response Team

ISMS Information Security Management System

ISO International Organization for Standardization

IT Information Technology

ITIL Information Technology Infrastructure Library

ITO Information Technology Outsourcing

M2M Machine to Machine

MSS Managed Security Services

MSSP Managed Security Service Provider

NIST National Institute for Standards and Technology

OODA Observe, Orient, Decide, Act

PII Personally Identifiable Information

RID Real-Time Inter-network Defense

SERT Security Emergency Response Team

SIEM Security Information and Event Management

SLA Service Level Agreement

SOC Security Operation Center

STIX Structured Threat Information Expression

TAXII Trusted Automated Exchange of Indicator Information

Chapter 1
Introduction

Today's evolving Information and Communication Technology (ICT) environment requires connecting not only new applications and devices, but also new providers and partners. As a result the ICT environment has been gradually outsourced to third parties, expanding the security perimeter. Some organizations are moving their ICT infrastructure to the cloud, where the options for incident response are either null or depending on third parties, with legal and accountability issues. Moreover, attackers (motivated, skilled and well-funded) are discovering new attack vectors, while defenders have to take care of multiple technologies and keeping them and themselves updated.

Incidents will occur sooner or later. What is important is to detect, contain and eradicate the incident quickly and effectively to reduce the impact to the organization. However, organizations under-invest on prevention and suffer from scarcity of skilled personnel. An evolving threat landscape and the lack of expertise in many organizations require new strategies to balance the need to manage incidents effectively.

Some companies provide outsourced monitoring and management of security devices and systems. Outsourcing incident management services seems to be a cost-effective way to satisfy some requirements from both small and large organizations. These kinds of providers are able to see a big picture view, by using the knowledge acquired by their solutions to their advantage.

1.1 Objectives

This thesis project aims to identify current practices to perform incident management through outsourced services. The outcome of this study will develop new awareness of the challenges posed by relying on outsourced services for incident management, such as prevention, detection and response. The research questions are:

- How do outsourced incident management services benefit or affect current incident management teams?
- How are roles, responsibilities and penalties described in service level agreements between a customer and the outsourced incident management service's provider?
- Which challenges are experienced during the implementation of these services in incident management?
- What are the future needs for outsourced incident management and what is lacking from the industry to make it real?

1.2 Outline

Chapter 2 introduces qualitative research and what it involves, the process of selection for the research method and the case study process followed in the present study. A background study of outsourced incident management services is presented in Chapter 3, where related published standards and guidelines are described and analyzed. This chapter presents a comparative summary of incident handling phases in standards and guidelines; it also describes the relationship between incident management, incident handling and incident response. Furthermore this chapter describes the MSSP categorization and the incident management services offered by the most significant providers in the market. Finally, Chapter 3 describes briefly situational awareness, the OODA loop, the intrusion kill chain model and their relationship to incident management.

Chapter 4 describes the organizations and experts in the case study. The findings from the case study are detailed in Chapter 5. Chapter 6 discusses the findings described in Chapter 5 and compares them with the background study described in Chapter 3. Chapter 7 presents the conclusions from this project and introduces future work.

Appendix A contains the request for participation in research project provided to the case study participants. In Appendix B the Interview guide can be found. Appendix C includes the notification receipt provided by the Norwegian Social Science Data Services. Appendix D contains the paper submitted to CloudCom 2015 conference.

Chapter 2
Method

The goal of this project is to identify the challenges on relying on outsourced services for incident management when incident management is performed in practice.

This chapter describes the research method used to approach the current experiences, researched in this thesis, as well as the reasons for selecting this method.

2.1 Qualitative research

Qualitative research covers a set of techniques which seek to understand a phenomenon, exploring specific issues and finding answers to questions. Merriam [Mer14] describes four key characteristics to understand the nature of qualitative research: "the focus is on process, understanding, and meaning; the researcher is the primary instrument of data collection and analysis; the process is inductive; and the product is richly descriptive."

Robson [Rob11] describes the key features of qualitative research as:

- Findings are not based upon numerical form but verbally.
- Context is important to understand the phenomena.
- Situations are based on the experience of those involved.
- The design of the research is an ongoing process.
- It has a holistic perspective and generalizations are not a major concern.
- It occurs in an ordinary framework.
- Does not require large-scale research in terms of persons or situations.

METHOD	(1) Form of research question	(2) Requires control of behavioral events?	(3) Focuses on contemporary events?
Experiment	How, why?	Yes	Yes
Survey	Who, what, where, how many, how much?	No	Yes
Archival analysis	Who, what, where, how many, how much?	No	Yes/No
History	How, why?	No	No
Case study	How, why?	No	Yes

Figure 2.1: Research methods, based on [Yin13]

2.2 Choice of method

Selecting the appropriate research method can be done using three criteria: form of research question, whether there are requirements of control over behavioural events and whether the study focuses on contemporary events. Yin [Yin13] explains that the first and most important criterion to select the appropriate research method is to identify the form of research question being asked. Then a further distinction among the research methods is based on control over behavioural events and the focus on contemporary events.

In this project, the form of the research question is a so-called ”how” question, as presented in Section 1.1. A further distinction among experiment, history and case study was determined by having no control over behavioural events and by focusing on contemporary events, since the project aims to identify current practices. Figure 2.1 illustrates the various research methods with the three criteria to determine the appropriate research method. As a result, case study appears as the most suitable method for this project, which is emphasized in the figure.

2.3 Case study

A case study is described by Yin [Yin13] as ”an empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context may not be clearly evident”. It is performed to study a real-world case gaining a deep understanding looking at it in context, relying on multiple sources of evidence and taking advantage of theoretical propositions to lead data collection and analysis. A case study includes 6 phases that can be repeated until the goal is achieved. The phases are plan, design, prepare, collect, analyze and share. See Figure 2.2

The plan phase is related to establishing the research questions and choosing the case study as the research method.

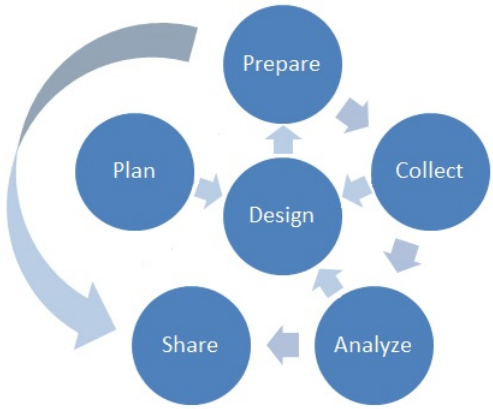

Figure 2.2: Case study research process, based on [Yin13]

The design phase consists of building a hypothesis about what is to be studied, linking the initial questions to the final outcome or conclusions and suggesting what should be considered within the scope of study. The purpose of this phase is to prevent the collection of data that do not focus on the initial research questions.

The collection phase addresses the importance of collecting evidence from multiple sources. Findings obtained from at least two different sources, providing corroborative discoveries are likely to be more accurate and convincing. The interview is described by Yin [Yin13] as "one of the most important sources of case study information".

The analysis phase involves reshaping the data in a preliminary sense or using a general strategy to identify what data is valuable and how should it be analyzed to extract observational conclusions.

The share phase consists of the preparation and edition of the case study report, in order to produce and expose the findings and conclusions.

2.4 Qualitative interviews

Hesse et al. [HBL10] define the qualitative interview as the process to "seek knowledge from the responder's point of view". To get in-depth and detailed information about the responder's experience, a qualitative interview is flexible and makes use of open questions.

There are several types of qualitative interview; the one selected for this study is referred in the literature [Wen01] [MN07] as semi-structured interview.

In a semi-structured interview, the researcher prepares, in advance, some questions which are designed to be open. This script is prepared having in mind that the responder's responses can't be predicted, demanding some improvisation for the subsequent questions during the interview. Semi-structured interviews must be planned and prepared beforehand; they demand discipline and creativity during the session, and require time for analysis and evaluation after the session. The interview guide used as a sketch can be found in Appendix B.

The interviews were performed via Skype or using conference bridges. All of them were done in a limited period of time. During the interviews, the responders addressed some initial questions, in order to initiate a process shift into a fluid conversation around the main topic of the interview and obtaining more elaborative answers

2.5 Document study

In order to enhance the knowledge gained through the interviews, relevant standards, guidelines, frameworks and academic literature was studied. This was a critical factor to develop a categorization of the outsourced incident management services and to address their challenges during the analysis phase.

2.6 Qualitative data analysis

There are various approaches to qualitative data analysis (See Table 2.1). The one selected for this study is referred to in the literature [HBL10] [Tho06] as the inductive approach. An inductive approach provides a set of procedures to condense raw data into a summary and establish links between the latter and the research objectives, in order to produce reliable and valid findings.

During the qualitative data analysis process the data analysis was guided by the research questions. The raw data was prepared in a common format and read in detail to get familiar with its content. Then a set of categories, based on key themes, were developed from the raw data. Thereafter a continuous revision and refinement of the category system was performed, including contradictory points of view and new insights. Finally, the framework containing the most important categories was constructed.

The findings of each case are presented in Chapter 5. A summary based on the experiences revealed by the analysis is given in Chapter 6.

	General inductive approach	Grounded theory	Discourse analysis	Phenomenology
Analytic strategies and questions	What are the core meanings evident in text, relevant to evaluation or research objectives?	To generate or discover theory using open and axial coding and theoretical sampling.	Concerned with talk and texts as social practices and their rethorical or augmentative organization.	Seeks to uncover the meaning that lives within experience and to convey felt understanding in words.
Outcome of analysis	Themes or categories most relevant to research objectives identified.	A theory that includes themes or categories.	Multiple meanings of language and text identified and described.	A description of lived experiences.
Presentation of findings	Description of most important themes.	Description of theory that includes core themes.	Descriptive account of multiple meanings in text.	A coherent story or narrative about the experience.

Table 2.1: Qualitative analysis approaches [Tho06]

2.7 Participants

The participant organizations is this study are transnational organizations selected based on the managed security service provider's (MSSP) market presence. The participant further described as Expert 1 was selected due to his expertise and experience in incident management, incident handling and incident response through different sectors as well as his role as instructor in a private company that specializes in security training.

A description of the participating organizations is presented in chapter 4.

2.8 Ethical considerations

The purpose of the research was informed to the participants during the interview request. Then each participant received a request for participation form asking for their consent, describing exactly what were they participating in and how their personal information would be handled. The request for participation form provided to the case study participants can be found in Appendix A.

The participation was voluntary with the possibility to withdraw at any moment. All information that could lead to the identification of individuals or organizations was anonymized or deleted. All participating organizations mentioned in this project were named using alias names. A secure erasure was performed to all recordings when the project was concluded.

The project was reported to the Norwegian Social Science Data Services.[1] See Appendix C.

2.9 Methodological challenges

A small number of organizations were studied due to time restrictions. The data collection process was performed through interviews. Interviews require active listening and formulating questions. However, posing "why" questions during the interview could lead to defensiveness from the participants. The challenges with the interviews should be considered. The ones present during this research were:

- Finding the right participant organizations.
- Requesting for remote interviews to transnational enterprises in a short range of time makes it difficult to get them.
- Re-scheduling interviews due to last minute difficulties in the participant's job duties.
- Limited time for the interviews makes difficulties to produce a fluid conversation around the main topic of the interview in order to obtain more elaborative answers.
- Limited time for the interviews could lead to leave out relevant information.
- Participants were interviewed remotely at their offices or meeting rooms, distractions such as emails, phone calls, text messages and more could have been present.

[1] http://www.nsd.uib.no/nsd/english/

Specific challenges related to the interview process for this case study were:

- Finding contact information from people inside the organization involved with tasks related to outsourced incident management services.
- Not all participants accepted to be recorded, which led to a challenging collection of data in those cases.
- Arranging interviews in different time zones.
- In most of the cases, the participants provided answers exalting their business model as a result of their economic interest to attract more customers.

Chapter 3
Background study

This chapter presents significant background information in relation to outsourced incident management services. An overview of relevant academic literature is introduced.

3.1 Related Work

The term incident management refers to the actions and mechanisms used to manage information security incidents. It is used to describe the collection of tasks involved with the incident response life-cycle. These tasks include planning and preparation, detection and reporting, assessment and decision, responding, and learning to prevent future incidents.

Different standards, guidelines and frameworks have direct and indirect remarks on incident management. Those that are most notable among the information security community are: NIST SP[1] 800-61 [CMGS12], ISO/IEC[2] 27035 [ISO11], ENISA[3] Good Practice Guide for Incident Management [MRS10] and ITIL[4] [Bri07]. These standards, guidelines and frameworks will be described in section 3.2.

Siepmann [Sie13] describes outsourcing as contracting out services, previously performed internally, to a third party. Both the third party and the organization contracting out the services take part in a contractual agreement that involves payments, and exchange of services.

A great amount of academic literature related to incident management and managed security services (MSS) has been published. Nevertheless, the literature focused on outsourced incident management services is scarce.

[1] National Institute for Standards and Technology Special Publication
[2] International Organization for Standardization/International Electro-technical Commission
[3] European Network and Information Security Agency
[4] Information Technology Infrastructure Library

Siepmann [Sie13] presents an analysis on security and privacy impacts when outsourcing Information Technology (IT) processes as well as recommendations on outsourcing preparation.

Sherwood [She97] studied the concerns regarding security of information within outsourced settings. The study presents a strategy to manage information security on outsourced technical services.

The study performed by Tøndel et al. [TLJ14] on current practices and experiences with incident management, identified outsourcing scenarios as one of the challenges for incident management. In accordance with their study, there is a need for improved understanding of the challenges of incident response in outsourcing scenarios particularly when several suppliers are serving the same customer.

Maj et al. [MRS10] discuss the outsourcing of incident management from the Computer Emergency Response Team (CERT) point of view. They suggest hiring the right people to guide the outsourcing process since it is a challenging project that should not be underestimated. Maj et al. recommend keeping control over the incident handling services and not outsource those elements of incident handling that provide control such as incident reports, registration, triage (including verification and classification) and the overall coordination of incident resolution. Some of the reasons given to outsource incident management related services are [MRS10] [AGM+03] :

- Cost.
- Lack of in-house skills.
- Physically hardened facilities with state-of-the-art infrastructure.
- Enterprise-wide management of security strategy.
- Access to global information on threats and countermeasures.
- Global prosecution on cyber-attacks and data breaches.
- Service performance 24x7.
- Particular services that you might not want to provide yourself.

In a previous work [Rey14], the author described that there is a need for research around the topic of outsourced incident management since it is a recent trend. The current available literature does not address it.

Siepmann's work [Sie13] addresses management of information security incidents but his comments only consider on managing incidents in outsourcing settings and not

managed by a trusted third party outsourcing the services. Sherwood's study on management of security on outsourcing contracts [She97], does not have an assessment on incident management. Tøndel et al.'s study on current practices and experiences with incident management [TLJ14] do not describe any outsourced incident management experiences or practices. The good practice guide for incident management published by Maj et al. [MRS10] only addresses outsourcing of incident management from the CERT's perspective. The author's previous work on incident management in outsourcing [Rey14], does not address the outsourced incident management model.

The present layout of incident management is trying to reach the capabilities to address today's evolving threat landscape and the gradual changes on the ICT infrastructure moving to the cloud computing. Through the process of studying the related work, the need to study the outsourced incident management services became evident.

The term CERT was used for the first time by the Computer Emergency Response Team – Coordination Center (CERT-CC) at Carnegie Mellon University. Some teams around the world took the CERT term and other teams used the term Computer Security Incident Response Team (CSIRT) to point out the task of handling computer security incidents instead of other technical support work. The terms CERT, CSIRT, Incident Response Team (IRT), Computer Incident Response Team (CIRT) and Security Emergency Response Team (SERT) have been used interchangeably in the literature to refer to teams that aim to mitigate the impact of a potential major information security incident.

3.2 Standards and guidelines

This section introduces some standards containing information regarding incident management. Each one of them is summarized. However, all the technical details of each option are not presented, neither which options are best is addressed, as that highly depends on the use case.

3.2.1 NIST Special Publication 800-61

This standard [CMGS12] aims to assist organizations in mitigating risks from computer security incidents by providing guidance on establishing incident response capabilities. It includes guidelines on building incident management capabilities and the interaction with external parties, such as vendors or Computer Security Incident Response Team (CSIRT).

NIST SP 800-61 describes in detail the four major phases of the incident response life cycle. These phases are (See Figure 3.1):

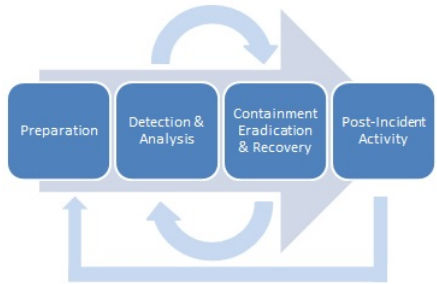

Figure 3.1: NIST Incident response life cycle, based on [CMGS12]

- Preparation.
- Detection and Analysis.
- Containment, Eradication and Recovery.
- Post-Incident Activity.

Preparation This phase involves everything that is needed to establish an incident response capability and to prevent incidents. Even though the latter is not a typical task for an incident response team (IRT) it is fundamental to the success of the organization's incident response capability. Preparation activities involve development of policies, procedures and response plans, provisioning tools and resources that may be valuable during incident handling as well as having multiple (separate and different) communication and coordination mechanisms. Prevention activities involve practices for securing networks, systems and applications. Some recommended practices are risk assessments, host security, network security, malware prevention and user awareness.

Detection and analysis Organizations should implement mechanisms to detect incidents and determine the potential impact that these may have. The detection might be the most challenging part of the incident response process. This phase involves automated and human detection capabilities. The guideline describes two categories of signs of an incident: precursors and indicators. These are defined as: "A precursor is a sign that an incident may occur in the future. An indicator is a sign that an incident may have occurred or may be occurring now". All the information collected and reported during this phase can't be guaranteed to be accurate. It should be evaluated to determine if it is legitimate in order to use it for making assessments and decisions. When the IRT suspects that an incident has occurred, it should document and time-stamp every step taken from detection to resolution,

since such information could be used as evidence in the case that legal prosecution is pursued. Incidents should be prioritized based on relevant factors, in order to handle them accordingly. Some factors that can be used to prioritize the incidents include: functional impact of the incident, information impact of the incident and recoverability from the incident. Combining the information from the first and second mentioned factors is possible to determine the business impact of the incident.

Containment, Eradication and Recovery Containment is important to prevent that an incident increases damage. It provides time to establish an ad-hoc remediation strategy. Containment strategies differ depending on the type of incident. Once an incident has been contained, eradication may be required to remove elements related to the incident. For some incidents eradication could be performed during recovery. In recovery, systems are restored to normal operations and vulnerabilities are remediated to mitigate similar incidents.

Post-incident activity This phase is a very important part of the incident response but usually omitted. It consists of analyzing the incident, including the actions taken in order to generate lessons learned. Lessons learned meetings should focus on revealing weaknesses during the recovery, successful approaches to mitigate the incident, corrective actions to prevent future similar incidents and resources needed to detect, analyze and mitigate incidents in the future. The purpose of this phase is to improve the security measures and the incident response life-cycle.

3.2.2 ISO/IEC 27035:2011 Information security incident management

This standard [ISO11] provides guidance to incident management. It offers a structured approach to deal with incidents including planning, detecting, responding and thereafter extracting lessons learnt. ISO/IEC 27035:2011 presents five phases with recommended activities. These phases are (See Figure 3.2):

- Plan and Prepare.
- Detection and Reporting.
- Assessment and Detection.
- Responses.
- Lessons learnt.

The standard ISO/IEC 27035:2011 aims to assist organizations in satisfying the requirements for establishing, implementing, maintaining and continually improving

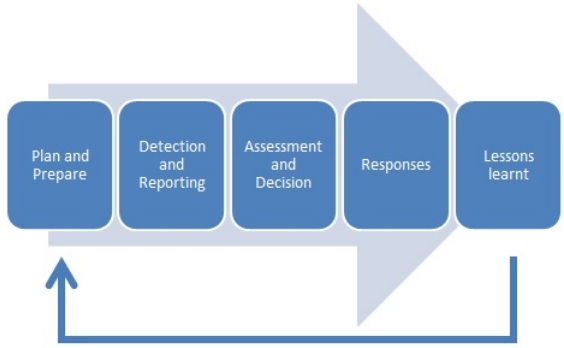

Figure 3.2: ISO 27035 Incident management phases, based on [ISO11]

an Information Security Management System (ISMS) specified in the ISO/IEC 27001:2013 – Information security management [ISO13a].

ISO/IEC 27035:2011 provides guidelines on the implementation of good practices on information security management presented in the standard ISO/IEC 27002:2013 Code of practice for information security controls [ISO13b].

3.2.3 ENISA - Good Practice Guide for Incident Management

ENISA's guide [MRS10] provides guidelines for security incident management. It provides recommendations on the creation of a CERT and assists on preparing its mission, constituency, responsibility, mandate organizational framework and the type of services, in terms of the incident management process, that can deliver.

This guide highlights the incident handling process, and provides related information on roles, workflows and policies. ENISA's guide pays no attention to the preparation phase and focuses on the incident handling process composed by four phases: detection, triage, analysis and incident response.

The relationship among incident management and incident handling is illustrated in Figure 3.3

3.2.4 The ITIL Framework

The ITIL framework [Bri07] is a source of good practice for service management that focuses on aligning IT services with the needs of the organization. The main goals of the incident management lifecycle are to reestablish a normal service as fast as possible and to reduce unfavorable impact on business operations. During the incident management process, resources are assigned to different activities such

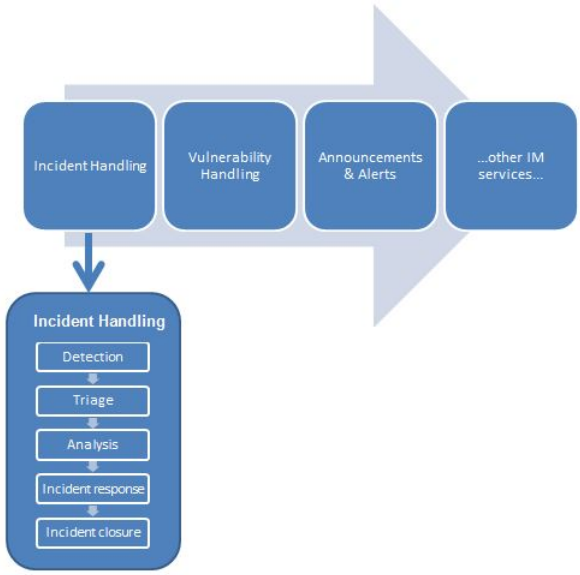

Figure 3.3: ENISA Incident management and incident handling relationship, based on [MRS10]

as identification, registration, categorization, prioritization, diagnosis, escalation, investigation, resolution, recovery, and incident closure, in order to mitigate and minimize the impact of incidents. The incident management process can be triggered by incident reports coming from diverse sources. See Figure 3.4.

The incident management process can be summarized in five phases: Identification and Logging, Classification and Prioritization, Investigation and Diagnosis, Resolution and Recovery, and Incident closure. See Figure 3.5.

The problem management process is a proactive and reactive process that involves preventing problems and resulting incidents from happening as well as eliminating recurring incidents. The problem management process is depicted in Figure 3.6.

In order to differentiate incident management and problem management it is important to describe that a problem is the underlying source of one or more incidents, whereas an incident always remains an incident. Its impact or priority may increase but it will never become a problem. Therefore, the main goal of problem management is to prevent problems and incidents, eliminate repeating incidents and minimize the impact of incidents that cannot be prevented. The incident management goal is to handle the incidents.

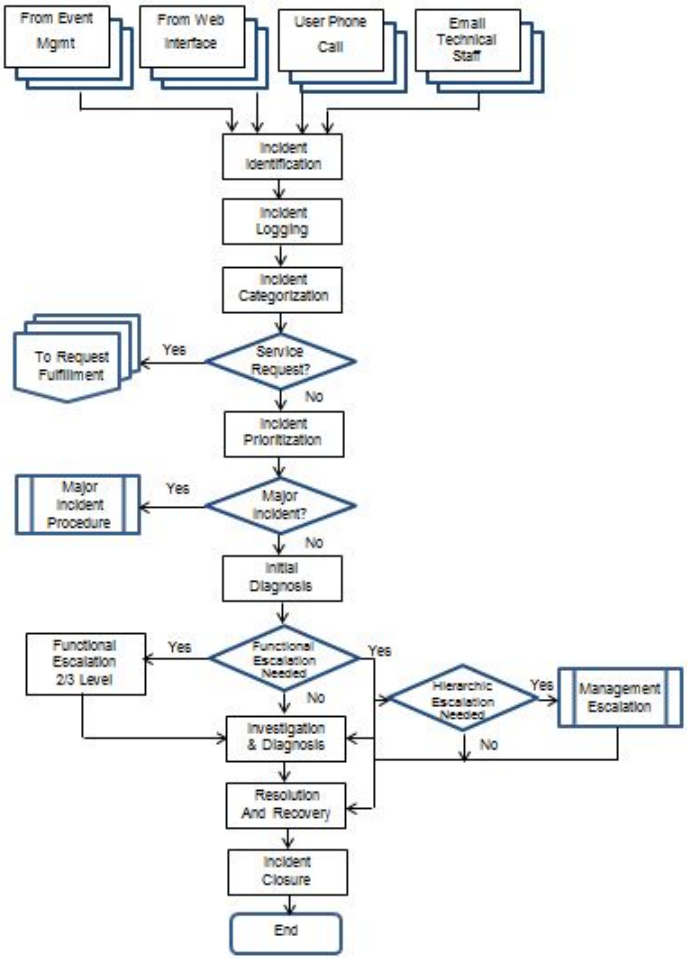

Figure 3.4: ITIL Incident management detailed, based on [Bri07]

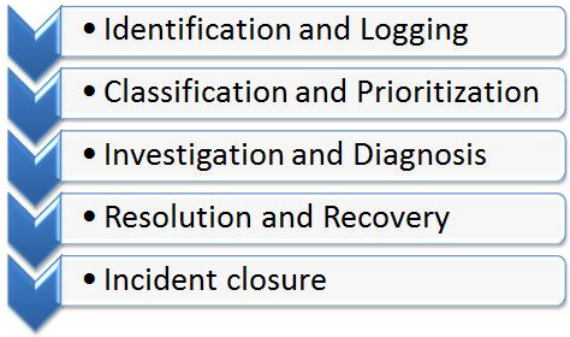

Figure 3.5: ITIL Incident management, based on [Bri07]

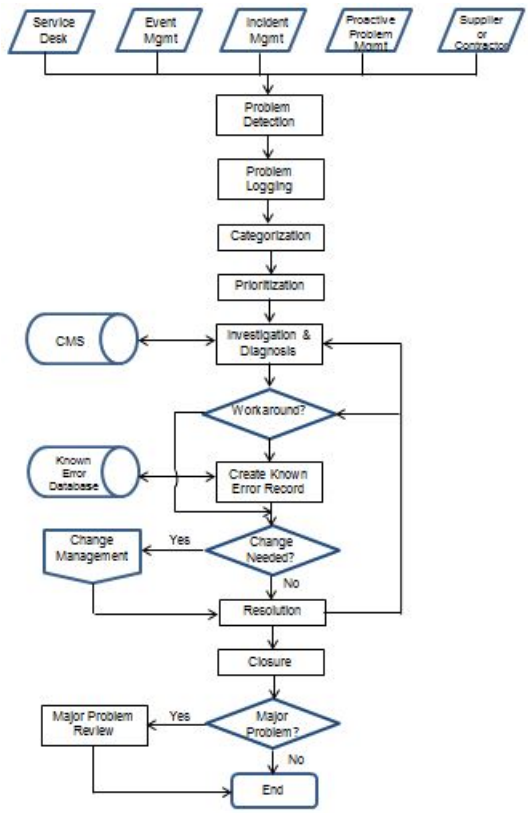

Figure 3.6: ITIL Problem management, based on [Bri07]

ITIL does not present the activities related to planning and preparation as part of the incident management process or the problem management process because it has reactive approach.

A comparative summary of the standards and guidelines described previously is presented in Table 3.1.

	Relevant phases						Focus
NIST SP 800–61	Preparation	Detection & Analysis			Containment, Eradication & Recovery	Post–Incident Activity	Proactive
ISO 27035:2011	Plan &, Prepare	Detection & Reporting	Assessment & Detection		Responses	Lessons learnt	Proactive
ENISA Good Practice Guide for Incident Management	–	Detection	Triage	Analysis	Incident response	Incident closure	Reactive
ITIL Framework	–	Identification & Logging	Classification & Prioritization	Investigation & Diagnosis	Resolution & Recovery	Incident closure	Reactive

Table 3.1: Comparative summary of incident management phases in standards and guidelines, based on [CMGS12], [ISO11], [MRS10] and [Bri07]

3.3 Incident management

There is a lack of consistency in defining incident management across the standards and guidelines as well as in the information security literature. The terms incident management, incident handling and incident response are in some cases used interchangeably. However, these terms have a different scope.

Incident management is part of a comprehensive security programme for information security governance [MRS10] [BBC06]. Killcrece et al. [KKRZ05] emphasize that incident management is not purely an IT issue, but a wide overview of the organization's security, risk and IT management functions. Alberts et al. [ADK+04] explains that incident management encompasses incident handling, incident response and a larger set of activities such as vulnerability handling, artefact handling, security awareness training as well as other proactive services and security quality management services.

Chichonski et al. [CMGS12] and Maj et al. [MRS10] present incident handling as a whole lifecyle where incident response is one of its phases. Incident response is an organized approach to react to a security breach or attack. The goal is to contain, eradicate and recover from the situation in a way that limits damage and reduces recovery time and costs. Figure 3.7 explains the relationship between incident management, incident handling and incident response. Where incident management has a broad scope of the organization's security functions and one of these functions is incident handling. Incident handling is a lifecycle from planning and preparation to the post-incident activites. The incident handling lifecycle contains incident response as one of its phases. Figure 3.7 is based on [ADK+04], [MRS10], [ISO11] and [CMGS12].

3.4 Incident management models

In a previous work [Rey14], the author classified the incident management models according to the organization's capabilities, human resources and expertise (See Table 3.2). The author described in that work that the outsourced incident management model is usually followed by organizations focused on their core activities or by organizations looking for cost reductions. The focus of this project is on the outsourced incident management model.

The incident management could be partially or fully outsourced in this model. Selecting a partially outsourced approach could be based on the lack of certain expertise or when is more convenient to use a third party to provide a particular service. On the other hand, fully outsourcing incident management would be an option for those organizations that want to focus uniquely and completely on their

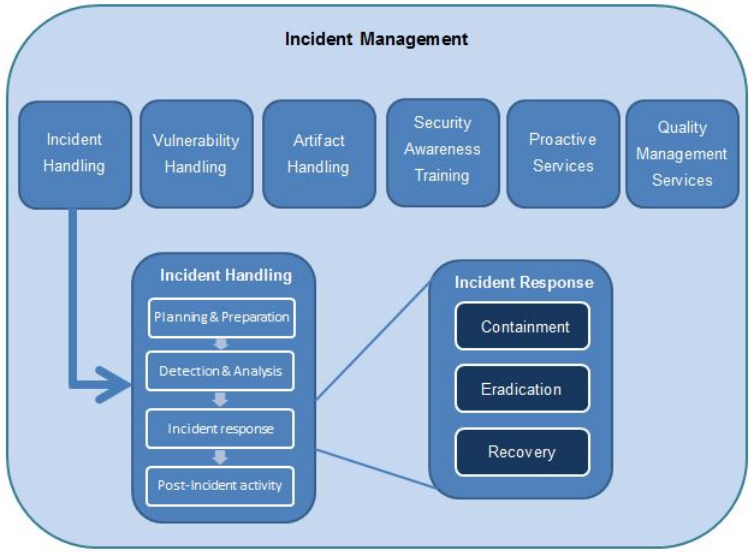

Figure 3.7: Incident Management, Incident Handling and Incident Response relationship

	Capabilities		
	At organization side	At provider side	Outsourced
Execution	Full-time Part-time Virtual team	Full-time Part-time Virtual team	Partially outsourced Fully outsourced

Table 3.2: Incident management models [Rey14]

core services and rather outsource anything else.

3.5 Managed Security Service Provider

Outsourcing incident management services is not an option that all organizations would consider, since it may be perceived as providing control and access to the digital assets. However, outsourcing incident management services is all about a security partnership with one or more trusted third parties.

Managed Security Service Providers (MSSP) supply organizations with expert teams and systems, improvement in performance, reduction in capital investment for technology and resources, and meticulous activities to exhibit to auditors and

Capabilities	Managed Security Service Providers (MSSPs)		
	Largest MSSPs (Enterprise-class)	Emerging MSSPs	Smaller firms serving the small business market
Security Operation Centers (SOCs)	Multiple SOCs in multiple geographic locations	One or two SOCs	Single SOC
Technology	Proprietary or significantly enhanced technology	Significantly enhanced technology	No threat intelligence services unless reselling another company's service
Portfolio	Full portfolio of standard services	Full portfolio of services	Narrow portfolio of services
Language support	Multi-language support	One or two languages	One language

Table 3.3: Managed Security Service Provider categories, based on [FH13]

regulators. A MSSP hosts, deploys and manages a security infrastructure, including remote and local security control while providing information security services.

Depending on the contracted services, MSSPs are able to provide support to the organization or (if existent) the organization's incident management team to manage incidents and to supplement or support the existing security infrastructure.

Ferrara and Hayes [FH13] categorized the MSSP in three categories, based on the size and capabilities of the firm. The first category involves the largest providers, also referred as enterprise-class. These MSSPs provide multiple security operation centres (SOCs) in multiple geographic locations, proprietary or significantly enhanced technology, full portfolio of standard services and multi-language support. The second category has the emerging MSSPs. These MSSPs have one or two SOCs, significantly enhanced technology, full portfolio of services and language support on one or two languages. Finally, the third category includes many smaller firms that serve the small business market. These companies have a single SOC, no threat intelligence services unless reselling another company's service, a narrow portfolio of services and support on a single language. See Table 3.3.

3.6 Managed Security Services

Managed Security Service Providers (MSSPs) provide a wide range of security services. Allen et al. [AGM+03] describe that the range of services, offered by the providers, differs in their ability to meet organization's security requirements, including, the availability, confidentiality, and integrity of information assets critical to the organization's mission. However, the current range of services offered varies according to the provider's ability to offer business and technical value.

There is no agreement on the type or description of the services being offered. Most of the providers offer similar or identical services, often using the same technology. However, each provider uses its own terminology to use a sales strategy based on differentiators. Throughout the literature [AGM+03], [ZXW09], [FH13], different lists of MSSP services can be found. However those services are not categorized. Schneier [Sch02] stated that "The field is so confusing that even the industry analysts can't agree on how to categorize the services offered".

Deshpande [Des05] and Ding [DYY05] each presented a categorization of the existent services at the time of their publications, but these categorizations are outdated and do not include many of the current services.

The following categorization is based on the services offered by some the most significant MSSPs in the North American market. The services are categorized in two main categories: Security IT outsourcing (ITO) and business process outsourcing (BPO). ITO services are performed commonly by MSSP's offshore locations. These services belong to the subcategory "Security enforcement & managed protection" and include managed protection services, cloud security, log management, database security, mobile device and machine to machine (M2M) security, and encryption services. BPO offerings are more refined and require robust process integration between the client and the vendor. BPO offerings are sub-categorized in exposure management, threat management and incident handling, identity and access management, risk and compliance management. Examples of services belonging to these subcategories can be found in Figure 3.8

The list of managed security services is expanding as demand for new security technology emerges. Table 3.4 contains a summary of the services offered currently by some of the most significant MSSPs.

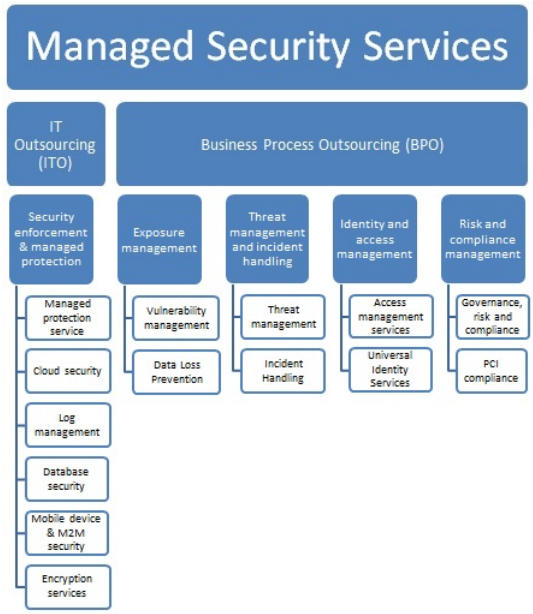

Figure 3.8: Managed Security Services

Service	Description
Managed protection service	24/7 monitoring of the perimeter network traffic through device management, such as IDS/IPS, firewall (traditional, UTM, nextgeneration, web application). Endpoint management providing automated patching for physical and virtual endpoints. Server management services including server protection firewall, server protection IPS and server antimalware. Web gateway management to protect the network from malicious threats through services such as gateway and enterprise client antivirus, email security, proxy servers and web content filtering. Netflow monitoring, which provides an automated collection and analysis of netflow data from the IP backbone network to discover indicators of compromise (IOC). Denial of service (DoS) and distributed denial of service (DDoS) protection to detect and divert potentially malicious traffic away from the network.

Service	Description
Cloud security	Security solutions that can be quickly deployed, fitting the cloud computing model delivering customer cloud security, cloud shared security and cloud provider security.
Log management	Managed security information and event management (SIEM) to monitor logs, correlate rule-sets, reviewing potential incidents and providing escalation of high-risk incidents. Log retention to collect and store logs generated everyday by critical information assets.
Database security	Database security protects databases against compromises of their confidentiality, integrity and availability, uncovering configuration mistakes, access control issues, missing patches or any other combination of settings that could leak to data leakage, unauthorized modification of data and other attacks.
Mobile device and machine to machine (M2M) security	Implementation of security strategies to take advantage of the benefits of mobility. Managing and securing the network of connected machines, devices, data and applications.
Encryption services	Digital certificates and PKI-based connection to extend recognition and public trust.
Vulnerability management	Internal and external vulnerability scanning assessment to find vulnerabilities identifying security liabilities across the network infrastructure, hosts and endpoints. Application defense and security assessment to find application vulnerabilities before someone else does it. Penetration testing services to detect, address vulnerabilities and uncover problems before they become serious. Application security code review to audit the source code for an application to validate that the proper security controls are present and the application works as intended.
Data Loss Prevention	Evaluation of the organization's data, classification based on its value and implementation of Data Loss Prevention (DLP) strategies to quantify risk and provide justification for improving security practices based on the value of the data and resources.

Service	Description
Threat management	Global threat intelligence providing in-depth analysis of emerging threats and zero-day vulnerabilities. Malware analysis and reverse engineering to understand the threat, its behavior and its impact to the organization, when a malicious code of an unknown type has affected the organization environment. Advanced Persistent Threat (APT) detection and protection through and active and layered defense model.
Incident handling	Emergency response services to provide support when a security breach occurs. Incident Response Plan development capturing roles and responsibilities of various stakeholders across the organization, preparing incident response processes and establishing communication flows and notification procedures. Digital forensics investigations to determine the root causes of incidents and provide evidence-based security protocols to prevent them from happening again. E-discovery services to preserve potential evidence during investigations avoiding potential legal matters and protecting the organization's reputation. Table top exercises to assess the response performance to threat scenarios.
Access management services	Access management services to provide appropriate rights and permissions accross systems and applications.
Universal identity services	Verification of user identities before accessing the IT infrastructure issuing credential to users quickly for secure login and access. Providing secure remote access to sensitive data to customers, partners and employees using mobile devices.

Service	Description
Governance, risk and compliance	Compliance monitoring measures compliance to a technical risk model by monitoring event logs not for intrusions, but change management. Risk management to establish critical baselines, evaluate security controls, identify regulatory holes, uncover process weaknesses and develop comprehensive strategies. Supply chain security services to validate that applicable laws and regulations issued by applicable governments and industry standards organizations are observed and complied. Consulting services provide tailored assistance in the assessment of business risks, security and security policies and processes development, and security product integration. Security awareness training to provide employees with a robust core of security knowledge to make the most informed decisions possible.

Table 3.4: Managed Security Services description

3.7 Situational Awareness

Endsley [End88] defined situational awareness as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future".

Situational Awareness is a core element to identify and detect threats early in any incident management effort. Situational awareness has the ability to be dynamic and respond to new and evolving threat models. In order to respond intelligently to the new threats, it is important to share data in near real time; and play an active role in providing the knowledge, capability, and capacity to secure and monitor the company assets.

Situational awareness has three phases: situation recognition, situation comprehension and situation projection. Barford et al. [BDD+10] and Albanese et al. [AJ14] defined the aspects of each one of these phases. The first phase, situation recognition, provides information about the status, attributes, and dynamics of relevant elements within the environment. The phase situation recognition requires being aware of the current situation and being aware of the quality and trustworthiness of the collected situation awareness information items and the knowledge-intelligence decisions derived from these information items. The final phase, situation comprehension, encompasses how people combine, interpret, store and retain information. Situation comprehension involves being aware of the impact of the attack, being

aware of the adversary behaviour and knowing why and how the current situation is caused. Situation projection encompasses the ability to make predictions based on the knowledge acquired through perception and comprehension. Situation projection requires tracking how the situations evolve and assessing plausible futures of the current situation.

Situational awareness aims to provide with the right information to everyone involved with the incident management and the incident response team, whether there are many incident responders and several compromised systems or one person examining one compromised system.

Situational awareness capabilities are insufficient today. Jajodia et al. [JNK+11] highlighted that there is lack of success on adapting to evolving networks and attacks, inability to transform raw data into cyber-intelligence and inability for handling uncertainty. A large number of alerts from network monitoring systems are often ambiguous and erratic. Real threats need to be quickly recognizable, understanding their potential impact in order to respond rapidly and accurately, mitigating them and minimizing the impact.

3.8 OODA loop

The stages of situational awareness are similar to the decision making cycle Observe Orient Decide Act (OODA) proposed by Boyd [Boy87]. The OODA loop is a continuous process composed by four phases (See Figure 3.9). Observe requires to collect data from the environment from relevant sources. The more that can be observed the more the attack can be understood. Orient involves using logic, expertise and learning to the data observed to understand what it means in context and enrich the knowledge on the current incident. Decide is where options are determined and the best course of action is taken. Act involves executing decisions effectively.

The OODA loop is a way to bring people, process and, technology together to defend against the cyber-threats. Klein et al. [KTM11] proposed to align all the different cyber-activities, related to the OODA loop in the cyber-defense context, holistically.

Companies need a holistic approach to cyber security, integrating multiple facets such as the threat actors, incident preparedness, legal counsel, anticipation of tomorrow's regulatory environment, compliance and a defensive strategy that continually adapts to the adversaries capability and threat landscape. The threat landscape is constantly changing and evolving, and companies have to monitor continuously for new vulnerabilities, new attack techniques, and anomalous or suspicious activity that might indicate a security incident is occurring. In the current cyber threat landscape,

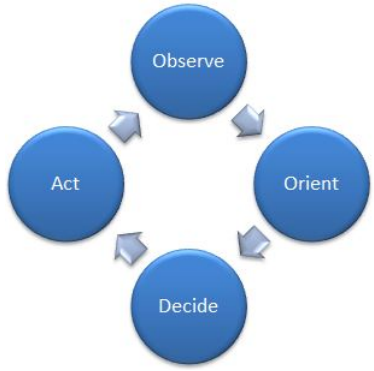

Figure 3.9: OODA loop

the OODA loop is an attractive framework for incident response management. When the OODA loop is implemented correctly, it touches all critical parts of the business, not just IT.

Gagnon et al. [GTK+10] describe that the OODA loop is used to achieve "decision superiority by making better decisions". It facilitates the observation and analysis enabling quick decisions and implementing new learnings in the next round.

3.9 Intrusion kill chain model

In addition, new techniques to defend from the unique aspects of the attack life-cycle are in development. The "intrusion kill chain" model, defined by Hutchins et al. [HCA11], is a model for framing an incident response analysis capability. It describes the phases in the development and deployment of a cyber-attack. These phases are reconnaissance, weaponization, delivery, exploitation, installation, command and control and actions on objectives (See Figure 3.10).

The kill chain analysis provides information on defensive courses of action. Detecting and analysing before the exploitation phase in the kill chain and implementing actions across it will change the defenders disadvantage of initiating response too late, which typically occurs during the conventional incident response process.

The kill chain model is effective for understanding defender's capabilities and performance facing highly complex attack scenarios. By understanding an intrusion and benefiting from intelligence during the early phases, defenders make the attackers modify every phase of their attack impeding them to reuse their strategies and using their persistence against them.

Figure 3.10: Intrusion kill chain model

Through this model, defenders can develop resilient mitigations against intruders and intelligently prioritize investment road maps to rectify any capability gaps. The effect of this model is a more resilient security posture when defenders align enterprise defensive capabilities to the specific model phases.

Chapter 4
Case Introductions

4.1 Case A

The organization studied in case A is an enterprise-class Managed Security Service Provider. Throughout the rest of this project, the organization in this case will be referred to as Organization A. The interviewees have a global public marketing role for security services and an investigation field operator role respectively. The first one has 6 years of experience with Organization A in the product marketing role. The latter has over 10 years of experience performing incident response and digital forensics.

4.2 Case B

The organization studied in case B is an enterprise-class MSSP. Throughout the rest of this project, the organization in this case will be referred to as Organization B. The interviewee has an account manager for service deliverables role and has over 17 years of experience with the organization through technical and management roles.

4.3 Case C

The organization studied in case C is an enterprise-class MSSP. Throughout the rest of this project, the organization in this case will be referred to as Organization C. The interviewee has a cyber security technologist role and has over 8 years of experience performing cyber security consulting, running sales and participating on managed security services' delivery projects.

4.4 Case D

The organization studied in case D is an enterprise-class MSSP. Throughout the rest of this project, the organization in this case will be referred to as Organization D.

The interviewee has a director of incident response role and has over 25 years of experience performing incident response.

4.5 Case E

The organization studied in case E is an enterprise-class MSSP. Throughout the rest of this project, the organization in this case will be referred to as Organization E. The interviewee has a director of cyber security services role.

4.6 Case F

The organization studied in case F is an enterprise-class MSSP. Throughout the rest of this project, the organization in this case will be referred to as Organization F. The interviewee has a security senior director role.

4.7 Case G

The organization studied in case G is an emerging MSSP. Throughout the rest of this project, the organization in this case will be referred to as Organization G. The interviewee is the manager of the threat intelligence and incident response team.

4.8 Expert 1

Throughout the rest of this project, the expert in this case will be referred to as Expert 1. The interviewee is an independent security consultant with more than 15 years of industry experience managing and securing networks in both public and private sector. He has instructed several training courses on penetration testing, intrusion detection and management of incident response teams.

Chapter 5
Findings

This chapter presents findings from the case study. Each case is presented separately. The collected data was prepared in a common format and categorized based on key themes. The information presented here is presented as given in the interviews. The quotations in this chapter are presented explicitly as given by the interviewees. The findings are organized based on three different stages: pre-operation, operation and post operation.

”Pre-operation” refers to the stage where an organization has not created a contract with any provider to acquire incident management services. ”Operation” describes the stage where there is a on going contract between the customer and the provider to outsource any kind of incident management services. Finally, the ”Post-operation” stage deals with a normal contract completion or an early termination.

5.1 Case A

This section describes findings from Case A, where the interviewees have a global public marketing role for security services and an investigation field operator role. Organization A is an enterprise-class Managed Security Service Provider.

5.1.1 Pre Operation

Organization A describes that the frequency of attacks and data breaches is increasing. The time that it takes for the attacker to compromise and get into the system or get to a piece of data that they want to get is very short. Minutes are usually what it takes for an attacker to exploit vulnerabilities and get into a system. On the other hand, the discovery phase, basically the victim’s time, to find out that it has been breached is usually taking months or sometimes even longer. In other words there are more attacks, it goes faster for the attacker to exploit and it takes longer for the victim to actually find out the attack and handle it themselves. Cyber-attacks are real, they are happening to everybody, no matter the industry. These attacks are

serious because companies are losing money, reputation, valuable assets, and all of this is crucial to their business. Therefore it is important that companies address this.

Organization A highlights that companies wake up to the security problem usually when either they have an incident or when the incident occurs to their competitor, to an organization or a company that is in their market, or in a country nearby. The companies hear about breaches in the news and then they think about not becoming part of the statistics, not becoming part of the news, and start wondering about: what can be done? How can they get protected against a certain attack that is in the news? There is a small fraction of the companies that are a lot more secure, such as financial services companies, governments or defense organizations that come up with a totally different background. They are more security aware, are typically deploying cutting edge security technology because it is simply necessary for them to effectively run their business. However, for most of the companies, being breached or attacked is what makes them look for what can be done about this issue. Those that get burned do not always talk about their breaches; they should do it in order to prevent other companies on the same market.

Some companies don't know what they want to protect, other companies don't understand why they want to protect it. These kinds of companies are usually not aware of what their threats are. Not all the companies have crossed this line since security costs a lot of money but there is no refund.

> *"Decision makers are not computer scientists, they are business oriented. Some of them think that if a breach cost them let's say 10 million but the latest security solution costs 20 million, not acquiring or contracting it will then be a 10 million saving. They prefer to take the decision of not setting the security controls in place because security does not bring them money back."*

Regarding the outsourced incident management services, Organization A describes that there is a lot of different stuff out there and everybody is talking about it differently. Some companies get an independent view, through a third party, of the players that are in the space to help them understand what their strengths and weaknesses are, and what might be suitable for their company to a certain extent. As a result, they create short lists of vendors that provide these kinds of services. After talking to different vendors, the companies get to a stage where it is not just about price, it is not just about the actual product or service to be delivered but in reality is about what is being delivered actually suits the company the best and it helps to

give them the peace of mind and the protection that is relevant and necessary for them.

Some companies have all sorts of tools in place that effectively gives them the information to be aware of and see what to expect from an attack, depending on the industry size and security awareness they have, but they are not viewing the logs or they are using the tools wrong. They are not monitoring them, they are not thinking about what a certain attack pattern can mean or they are not really customizing the tools for their company. This is because they often don't have the experience or they don't want to do it, therefore, they prefer to outsource these services. Companies typically don't want to focus on that, they want to focus on whatever is their business, what they are making money with, but not necessarily security.

Organization A describes that there are some MSSP's that help customers to manage devices and some other security services. Nowadays, there are so many logs coming from all sorts of tools. Customers in general really have a hard time aggregating and finding out what is admissible, what is not a risk for them and what, in a series of attacks, can harm them in a big way. There are also some MSSP's that offer different types of managed security services that not just manage devices but really help to monitor and analyze the incidents, manage the intelligence and the information that is gathered by the customer, the information that is gathered by the provider about what is going on in the world in terms of attacks, and the one that is available on the network to recognize and intercept an attack when there are indicators of compromise before it actually does harm.

> *"It is important to get the combination right, to have access to all the information and intelligence, and have the tools, the knowledge and experience to understand what is there when you look at it."*

Organization A's mindset, regarding the acquisition of a new customer that is switching its outsourced incident management services from one provider to another, is to help the customer the most and the best. Therefore the new provider needs to act as close and connected with the customer and with the previous provider as possible. The difficulty relies on understanding the business of the new customer, and on creating a trusted relationship. Understanding the business of the customer requires learning about the infrastructure that the new customer has, understanding what are the critical assets and what does the customer wants to protect. Building a trusted relationship between provider and customer is something that is done over time, in some cases years, over successful protection in terms of attacks and is built by and through the people and through the experts that interact with the customer.

5.1.2 Operation

Organization A considers that getting outsourced incident management services might become an issue for some companies with internal incident teams, because at the end of the day internal people are being replaced with a service from an external provider. As a result, there is reduction of staff, but the company gets a better and cheaper service from somebody else. This is the same effect as when companies outsource any service like payroll, financial services, cleaning services, etc., because companies tend to want to focus on their primary business.

Organization A emphasizes that in order to stop attacks before they do damage, customers should be able to understand what to look for, to have the appropriate tools and the experience to recognize certain patterns or types of incident, as well as to have the tools to alert about an attack before it actually does damage. These are the things that most customers struggle with, to stay aware of what the attack patterns are out there, to know what is going on in a global landscape and then to become proactive.

In some cases Organization A has detected through their incident management services some indicators of compromise (IOC) that indicate that something might be happening in the customer's network and as a consequence alert the customer, depending on the severity of the problem, Organization A might insist on taking actions or asking for authorization to investigate more, depending on the service level agreement.

> *"Sometimes an incident can go on for a long period of time. In some cases we (the provider) can have multiple times where we go back and forth. At some point the customer realizes that there is something that is not perceivable by itself, something that its software and tools were not alerting on. Then, the customer recognizes that is clueless about what to do in order to contain this problem. The customer doesn't know what to look for, and often time is very dependent on us (the provider) to get the issue resolved to get the attack stopped."*

According to Organization A, the combination of: multiple sources of intelligence, tools, the quality of the input that a provider can have access to and the experience have as a result a more mature response and less false positives for the customer.

Customers want to be protected against attacks or incidents that go after valuable assets and/or that are potentially damaging for them. These events are the ones that customers want to detect and there is where the provider's experience, intelligence and the quality of tools make a difference.

One of the challenges during the response is when the MSSPs are providing a service to a new customer that has never been in touch with the provider before, and the customer is looking for an incident management service as a consequence of a breach. There, the provider's incident response team sees the company's infrastructure for the first time. It needs to help very quickly and effectively, it is required to analyze the network, understand the data flow and the infrastructure. Once they find the breach, they have to work their way through the breach and through the systems, if cloud services are involved or the systems are located in different countries then it takes some more time to send the human resources to get the logs, if required.

Data breaches and cybercrimes are not only technical, companies can't fight them with only technical aspects. Technology is only one factor, but there are many more. That is why Organization A has ex law enforcement personnel, computer scientists, auditors, lawyers, etc., who can think outside the box about a breach.

When the customers have an incident and the MSSP's incident response team needs to get to the company, it might face different scenarios. One of them is that the customer has no incident management team. Then, if the company has no security preparedness there might be communication conflicts, because they might lack internal communication or knowledge about who to contact, how to do it or even long delays because the IT personnel handling the incident might not have top management support. On the other hand, the customer might have its own incident response team that would require from the provider's team only support with more man power, or support with specific tasks such as reverse engineering of malware. It depends on the local incident management team's capabilities.

Those who work for an internal incident response team do not get to see the big picture; they might see only incidents from their company. However, those who work for a MSSP have a vision of many breaches from all over the world, which allows them to correlate breaches from one company to the other.

Organization A's responsibilities and penalties in a Service Level Agreement (SLA) are really dependent on what the customer is looking for and is willing to pay. Typically for outsourced incident management services, there is a share agreement between the provider and the customer; there are different levels of incidents or indicators of compromise, different severity of attacks but at the end of the day, it is very much about what the customer is willing to pay for.

Everybody theoretically wants 100% security, there is no such thing but everybody wants a maximum security environment and not everybody needs it nor has the money to pay for it, nor is willing to pay for it.

A problem in real life for the providers is that many customers want services to be

implemented in mass and to be working without false positives, basically not being alerted for stuff that is not relevant. That depends on the quality of the services, but in the future, there will be more innovation into other IT systems, basically network systems and security systems would become integrated.

5.1.3 Post Operation

Organization A considers that customers switch from one provider to another because they are not having the service that their former providers said they provided or because the service is too expensive or a combination of both. There might be also cases where the provider was not able to help them, because they didn't see the attack coming and the customer's assets got affected.

5.2 Case B

This section describes findings from Case B, where the interviewee has an account service deliverable role. Organization B is an enterprise-class Managed Security Service Provider.

5.2.1 Pre Operation

Organization B describes that the cost reduction is the main driver for most of the companies that are looking for the possibility to outsource IT services. Depending on the quality of the services that will be outsourced, it will have an impact on the cost.

Organization B highlights that the communication inside organizations and companies should be considered. It is important to be aware that outsourcing services to global companies might impact the internal communication. People are used to communicate in their own language, but with the integration of outsourced services to locations with a cheaper labor cost, they will need to react and get used to talking to people in another language for example English.

Organization B considers that the staff morale has an important role if companies are considering outsourcing something that was previously run in-house. The staff needs to be involved, making them understand why the decision to outsource was made and try to make it positive. Outsourcing services do not necessarily means firing people. It could be that the people just needs to be re-skilled and reassigned to a different position within the company.

When Organization B submits a bid for a new client, people working within sales want to deliver a bid which is as good as possible, low cost and delivered as soon as possible. This looks very attractive for the client because there is a very competitive price and Organization B promises everything up and running within a short time

frame, faster than anyone else. However, when the deal is signed and the technicians, project managers and architects among others are going to start on their work they realize that is a lot more complex and not realistic to deliver it in the promised time frame. If Organization B is not able to perform the project with a new client within the given deadline, then all additional project costs are absorbed by Organization B until the project has been completed.

5.2.2 Operation

Organization B has implemented global procedures; it aims for fewer but larger service desks to support its clients. But some of the global procedures have reduced some short-cuts during the follow up process.

> *"It is not that easy to take the short-cuts that you were used to take earlier because you don't know the people who is actually working on the service desk any more, that was a lot easier when we have met before during meetings. I mean it was easier to get hold of them and maybe use some short-cuts if you needed some quick help. That is not as easy any more; we should follow the same procedure on the service desk anywhere in the world and is working quite good actually."*

Organization B has offshore centres in India and Lithuania. The resources situated in those locations have different type of rules. The service desk is located in Lithuania, while the offshore center in India handles incident management and problem management. Previously the service desk was located in Norway but based on a cost driven evaluation, it was moved to provide a global service desk for the Nordic region. The clients still call the same phone number, and can still talk to people who speak their language.

The cultural differences between India, Lithuania or the Nordic countries could be challenging for Organization B, because in India the resources are not as good to take decisions on their own, they need to be told what to do and that means that they are not working as independent as one would hope they would do.

> *"That is how they are used to work in India and I wouldn't say that it is a specific problem for Organization B, it is for all the companies that have employees in India. They are kind of reluctant to make their own decisions because if they make a bad decision, the impact could be bigger for them than for us. It is easier for them to get complains from the managers if they do something wrong compare to other countries."*

Organization B spends some time to follow up the resources in India because of the cultural differences.

> *"They don't think that much out of the box, they just follow what they have been told to do, while in the Nordic countries people try to think on their own and resolve the problem. A major improvement not only for Organization B but for all people working with offshore resources in India would be that the Indian resources become better at taking independent decisions and not just wait being told what to do. Sometimes you get tired of telling people what to do, even if they are a lot more skilled than you, because they are reluctant to make their own decisions."*

Organization B has locations in India at three or four different areas. Even though there have been few occasions where due to different circumstances like earthquakes, strikes, or riots people has not been able to get to work, Organization B has never experienced a problem within all the regions at the same time.

> *"Having these functions spread over different locations is a good way to spread the risk, if one location is somehow not able to get to work, we have resources at other locations that could assist until they are up and running again."*

Whenever Organization B's customers have an incident, either reported by the customer itself or detected by Organization B a ticket is raised and based on the information available a resolver group is assigned according to the incident priority. If it is high priority incident, a major incident management is gathered with the account team. Once the issue is identified the client is informed about it and about the troubleshooting performed. If the problem takes longer than expected, a time frame for updates is agreed and updates are provided until the problem has been resolved. Then the problem management team gets involved to find the reasons for the issue and to identify how future occurrences could be prevented. Based on that information improvements are designed or implemented. Everything gets documented. The documentation contains all the details from the problem registration to completion, updates during the troubleshooting, cause and preventive measures. There is a global process within Organization B for incident management and problem management. During the incident management, everything is documented to get as much details as possible into the documentation that is shared with the client. Then during a meeting with the client, all details are explained. The client might be happy with the documentation provided, if not the client would come with feedback that

would trigger a new follow up activity within Organization B to see whether there is something that could be improved in order to resolve the problem.

Organization B performs a proactive work with its clients to prevent the problems before they actually occur. Organization B has weekly technical meetings with the clients to discuss the updates and security patches that would be applied. By having this kind of meetings and also providing monthly reports the client perceives that Organization B does whatever it can do to make sure that the client's environment is safe in order to avoid any kind of incidents on their systems.

The penalties at the SLAs might differ from account to account. The more demanding SLAs the client want, the more they have to pay to Organization B, because it requires more staff. Organization B has different SLAs according to the environment (production, test, development, etc.). The SLAs related with the production environment have higher cost and penalties than the rest. However, Organization B has compensation agreements.

> *"If an SLA is missed and there is a penalty, the compensation could be used. If the following three months there are no more SLA penalties then the penalty that Organization B would have had to pay gets waived."*

When Organization B detects an incident, fast decisions must be made. First of all, the client is contacted to provide it with information on the incident and to explain what is recommended to do. Once the approach is approved or the client has provided input from its end and an agreement is reached, that information is passed within the internal Organization B's team that is handling that specific incident to resolve the problem.

> *"I am always trying to take the fastest way to get hold on the client. I can basically call the client 24/7 if we have any problems and I can discuss with her/him the approach that should be taken. Even though Organization B needs to make the changes, the client needs to take decisions. By me calling someone from the client directly I feel that I am really able to make decisions very quick and be proactive so that we can try to resolve the problem as soon as possible."*

5.2.3 Post Operation

Organization B describes that the client can always cancel the contract whenever it wants but there are some cancellation clauses. If the contract is ended before it expires then there is a fee that needs to be paid in order to get out of that contract.

Organization B has had a client which decided to look for another service provider once the contract expired. A transition project started to move the Organization B's infrastructure assigned to the client to the new vendor. The client had to pay for everything that had to do with the transition. Most of the challenges were actually for the client and the new vendor. Once the transition project started was when the client and the new vendor actually realized how complicated things are. Organization B needs to handle documentation to the new vendor about the systems that provide support for the client.

The problem is similar when a new client is changing provider to Organization B. It is difficult to transition all the servers, infrastructure and to get the problem knowledge. It is more difficult for the service provider that is taking on with the service and it is easier for the provider which is handing over an existing infrastructure.

> *"The client often forgets how complicated is to actually rent and maintain an environment. And it seems like the client does not realize about that until is moving everything to another vendor. Then the client understands how complicated things are and how many things can go wrong. But by that time it is too late, because they have already signed an agreement with a new vendor."*

Organization B describes that sometimes it can be difficult to get the information from the previous vendor because it might be reluctant to give that information easily; it is knowledge that took many years to get. So they do not give anything to Organization B automatically. However, Organization B behaves similarly.

> *"We give them all the information that we are obliged to but maybe we do not tell them all the bits and pieces with the knowledge that we only have in our own head and that it is not documented."*

In some cases it gets more complicated. Organization B had a client for 10 to 15 years that decided to change provider. The transition project has now been delayed for about a year because the new vendor sees that this is a lot more complicated than what it was assumed originally. As a result, Organization B has actually signed a new agreement with the client for a number of the deliverables, not everything. Then, the client was so unhappy with the new vendor that Organization B won back part of the deliverables. The new vendor did not have all the knowledge and skills to run and maintain everything the client wanted. That is not because Organization B did not give to the new vendor the information. It was more complex, more difficult to run and maintain than may be what it was assumed when the client and the new vendor signed the agreement.

5.3 Case C

This section describes findings from Case C, where the interviewee has a cyber security technologist role. Organization C is an enterprise-class Managed Security Service Provider.

5.3.1 Pre Operation

Organization C recommends that when any provider offers services they should be clear about where these services are located in the incident management process, where the starting point is, where the ending point is and what are the resources required from the customer in order to implement the services.

> *"Every provider tries to differentiate their services compared to somebody else. Some may decide to market whatever they do in a slightly different way to try to gain a competitive advantage. I don't know if we will ever have a universal agreement on the nature of the services."*

Organization C describes that there is a lot of confusion about the services offered, since some providers label things differently so that they can serve as a differentiator for them. Customers are trying to figure out what exactly is the service provided, whether the service is provided at their facilities or remotely and what are the changes needed in order to implement the services provided.

Organization C highlights that it is important to understand the customer expectations, especially when the customer is switching from one provider to another, as well the expectations that were not met by the previous provider. The provider needs to understand the new customer's challenges in order to identify the services that can be offered in that category and propose something based on it, response times, types of skill sets that can be provided, or a set of services based on their prior experience.

5.3.2 Operation

Organization C has very specific SLAs for incident reporting or detection based on its severity. If there is an incident or suspected incident there is an escalation process to notify the costumer, which is done by phone or by other means based on its severity. The customers can watch and look back over the history in order to understand what happened and how they were notified during the incident detection phase. However, Organization C uses a different set of SLAs when it comes to incident response.

> *"I think it is somewhere unrealistic to have very specific response times, particularly for a large customer. Response times can vary depending on their geographic location and the nature of the skills needed."*

Regarding SLA's responsibilities and penalties, Organization C describes that the nature of both the costumer and the provider should be understood. It is important to consider what is being offered and what the consequences are for the customer if that service is not offered.

> *"Most vendors are not willing to take a lot of liability for something that is unpredictable as responding an incident."*

Pre-paid services commonly involve an agreement between the provider and the customer to provide a service on-demand guaranteed by a fee payment established on the agreement. Pre-paid services, with clear obligations and penalties, certainly helps to guarantee financial consequences for any failure to meet the SLAs. However, it is probably unrealistic to expect any serious penalties beyond a few free hours or something else that may be offered in compensation for the failure, eventually the ultimate penalty is that the customer chooses to go elsewhere. It tends to get people sufficiently motivated in some cases to not lose clients.

> *"When a customer chooses to go elsewhere it becomes your guide in terms of whether or not you meet the expectations even if it is not written in the contract."*

Organization C describes that even when companies outsource incident management services, the companies still need to have legal and human resources inside the organization that need to be involved when there is an incident. Legal advisors need to decide when you are obligated to report, stakeholders need to define what they communicate to the media and to their customers, as well as the process by which they do that.

Organization C explains that planning and defining roles and responsibilities is very important especially for those companies that aim to do a comprehensive outsourcing. Defining physical and logical access credentials prior to an incident is essential in order to prevent delays during the investigation and remediation process, alerting and reporting responsibilities should be well defined so that the expectancies would be unambiguous.

Current customers might also choose to engage Organization C in services not acquired before, when they are going through an incident. The engagement tends to be due to the incident, not necessarily an ongoing service. In those cases Organization C responds to the incident, and since there is already a contract in place, the engagement gets priced in. However, Organization C gets approached also by new customers who suspect of a security breach.

> *"The challenge there is to be able to respond quickly enough, get a contract in place, get somebody on site and be able to access whatever device is expected to be compromised, and investigate the breach."*

Having prepaid service might be easier from the contractual standpoint but there is still the issue of making sure that the contract of those provided services have people available to respond as needed, since the personnel might be actively engaged in different tasks. Then it becomes a staffing issue of being able to provide the appropriate people at the appropriate time. A lot of customers may choose to have multiple vendors engaged in a contractual relationship, or something similar, to call at the moment of need, expecting all of the providers to jump in the action.

Customers may have multiple providers but usually only one is engaged in at any given time. The interaction between multiple providers might happen from time to time in some of the bigger incidents, but there is some sort of hierarchy involved, so that they can make sure that somebody is in charge. In some cases there are different providers supporting the same incident, and even when they are all doing different things, there can be some overlap.

Many customers are just simply interested in getting everything back, up and running and removing whatever it affected them. In terms of how far an incident is investigated, it is always dictated by the customer. It is the customer's decision to pursue it further or not. Some of the customers decide not to fully investigate because there are reporting obligations that they have to follow if Personally Identifiable Information (PII) is compromised.

Organization C explains that internal incident management teams might benefit from different areas of specialization. In some cases the incident management team might need specific services to improve their incident management plan and strategy, documentation and more. In other cases, the internal team might lack expertise in advance topics like malware analysis or reverse engineering. Finally, the internal incident management teams might have an appropriate expertise, both technical and managerial skills, but the incident might be too large or the team is also handling something else and more manpower is needed. Then they could get some services

from a provider in order to work side by side, sharing resources and adding specialized support.

It is important that the provider integrates well with the customer. If the customer relies completely on the provider, there will be some challenges with getting the customer's management up to speed and fully appreciating the nature of the incident. The customer is the one that is bearing the risk, and if it doesn't have qualified people; it is a lot harder to make decisions. On the other hand it can be difficult to integrate between two teams that are trying to respond in the same way. So having clear lines of responsibility in terms of who does what is certainly preferable.

There are different approaches to real time response such as the Observe, Orient, Decide, Act (OODA) framework. Independently of the approach taken, it is important to define clearly the roles and responsibilities of those observing, orienting, deciding and acting, because those activities performed by different parties might vary depending on who is having those roles.

> *"[OODA] is indeed a useful process but at each of those stages, it is important to have a clear role on who is observing and what are they observing, who is orienting and what are they orienting themselves against, who is making the decision and what are the actions based on."*

Organization C explains that one of the current challenges for MSSPs is to understand the customer's environment better. That means doing some work prior to an incident to first of all define the processes, the procedures by which the response is done, what the network looks like, what applications are run, where the critical assets are located, what does the organizational structure looks like in terms of who can authorize what, and more.

The best relationship between providers and customers is where the roles and responsibilities are clear, it is not necessarily better that the provider does everything, even though it is financially convenient. The provider just needs to make sure that the customer is not ignoring the risks and the decisions they need to make themselves. The risks can't be taken on behalf of the customer. It is their task to say, this asset is important and the provider can for example give advice about what should be done. However, it is the customer who has to face legal responsibilities if any loss of data, lawsuits from customers or loss of intellectual property is experienced.

Organization C highlights that the industry is still lacking better automation and better integration to address incidents. With better automation at the customer level, the easier it is for them to do many tasks themselves and the easier it is for a provider to come in and use those mechanisms. More integration of multiple incident response

tools is needed to offer more complete software packages, as well as integration from software vendor's products and MSSP's tools.

> *"Software vendors prefer to sell their products to end costumers than to service providers because they can get more profit through those sales. The software vendors are not always receptive to integrating with outside vendors and the tools they use."*

Organization C outlines that threat data and threat intelligence needs to be better integrated with the tools used for incident handling.

> *"We work hard in our organization to try to integrate threat intelligence data right directly into our security information and event management (SIEM) so that we can actually respond in real time to new potential attacks that are coming in."*

Some IRTs are providing tools that integrate data that they have collected from their incidents which can be used to be more proactive in responding to future incidents. But there is still more to be done to integrate threat intelligence with larger databases to be able to identify and stop threats before they have any impact.

5.4 Case D

This section describes findings from Case D, where the interviewee has a director of incident response role. Organization D is an enterprise-class Managed Security Service Provider.

5.4.1 Pre Operation

Organization D describes that the incident response community has done a relatively poor job at defining terms and standardizing processes. This makes it difficult for those looking at outsourced incident management services, if they are not incident response experts, to fully understand what the services offered by MSSPs are. Organization D devotes time helping potential clients to understand how what Organization D does is different from what others do and what some of the differences in its proposal are.

Organization D outlines that Chief Information Security Officers (CISO) have difficulties to adequately plan financially for incident management services when an outsourcing provider would be contracted. It is hard for CISOs to have certainty in how much they will spend every year since it might depend on the type of contract,

the type of services, how many incidents the organization would have, their complexity and how long it takes to resolve them. For example, the budget for external services might be exceeded quickly during very large incidents.

5.4.2 Operation

Organization D considers that some organizations should find out how to effectively integrate an external party providing incident management services. On one extreme are those organizations that are overloaded at certain point of time and need help on doing services that they don't have time to do. On the other extreme are the organizations that need the outsource partner to provide all the resources that are necessary from both a technical and non-technical perspective to resolve the incident. These are the two extremes and usually every organization outsourcing incident management services falls somewhere between the two of them. According to Organization D, the latter case is the most difficult case to integrate in an organization, because people that are potentially not familiar with the organization, who don't know who all the players are, they have to learn about it on the fly. These difficulties can delay the response to an incident.

Organization D manages the engagement with their customers considering the nature and size of its client. Small businesses might be more dependent on the provider to manage almost everything related to the incident, whereas larger businesses which have their own security teams may supplement their existing staff with the provider's help. In both small and large businesses, there is a lot of fear in the employees today when it comes to incidents, because people are fired every day due to handling them improperly or not being able to contain them adequately.

> *"Customers with incident response roles fear to get fired when an incident is out of control; there is when they feel that the outside provider can help them manage something in the right way so that they don't get fired."*

Organization D devotes time with the customers to understand not only what is happening during an incident but what it is exactly the customer's need from Organization D in order to help them to deal with the incident.

Organization D describes that it provides, in its contracts, descriptions of each service, as well as service level agreements for those services. These SLA's define how soon actions for response would be provided, such as the time to get someone on the site.

Organization D considers that customers can significantly improve their preparedness and their response time for incident response services if they start collecting the correct data and instrument appropriately their network and systems. The biggest problem that providers encounter technically when responding to an incident is the fact that most organizations are not collecting sufficient logs and data to facilitate the incident response process. If customers would collect the correct information and store it for sufficient time, it would significantly speed the response and could even allow some response functions to be performed remotely to avoid waiting for someone to actually get on site and to start searching for what is happening on the network or the infrastructure.

Organization D describes that customers can evaluate threat intelligence by finding out how intelligence is collected by the company, asking a series of questions such as what are their sources, what are the capabilities of the people that are performing that function, and more. The other way to do it is to either purchase the service for a short period of time or get samples and compare information between providers to determine the best option according to what is actually needed.

Regarding remote response, Organization D comments that IT departments in general don't like agents because every additional agent creates the potential that there is going to be problems that the IT department is going to have to deal with. Generally the CISO or the decision maker has to convince the ultimate decision maker, whether is the IT manager, the Chief Information Officer (CIO) or someone else, that the value of having an agent running on an endpoint is greater than the potential cost that IT is going to potentially have by adding an additional agent. Organization D has worked with customers to help convincing their IT departments or their CIO as to why the benefit of running the agent at the endpoint is greater than the cost.

Organization D highlights that MSSPs have the same problems that companies have in hiring and retaining good talent. There is such a shortage of people with capabilities for incident response activities. It is difficult to hire as many people as is needed. Organization D is addressing this issue by hiring more junior talent and helping to train them. The new employees learn through training and in depth hands on experience.

> *"If you look at the available training, many of them help with very procedural types of functions but don't really help to understand the bigger picture and how the response to certain types of incident activity should be. That is still learned by people through experience."*

Organization D describes that incident response roles involve multiple roles that

are not clearly defined in the industry. The skills from those performing these roles can be to a great extent so different, that describing a person as an incident response expert, doesn't give a clear indication to what capabilities that person actually has.

Organization D is going through a process of defining what those roles actually are for its own needs, so that when hiring people, there would be a clear understanding about what they really have experience in and how that maps to what it is we need at any particular profile.

Organization D highlights that the NIST incident response model doesn't make sense any more because it handles an incident in a linear way. Organization D is a strong proponent of the OODA loop and believes that it would change the efficiency and effectiveness of processes.

> *"The OODA loop concept fits in well with the concept of incident response."*

5.4.3 Post Operation

Organization D describes that when a customer switches providers, then it is more challenging for the provider getting the new contract, especially when there is an incident in progress. The new provider has to catch up with the state of that particular incident. On the other hand, the provider losing a contract may not have much incentive to participate on the process and would probably do it only to the extent of what has been agreed.

5.5 Case E

This section describes findings from Case E, where the interviewee has a director of cyber security services role. Organization E is an enterprise-class Managed Security Service Provider.

5.5.1 Pre Operation

Organization E describes that customers have a very difficult time predicting how much resources or help they are going to need and justifying it within their business. There are moments where cyber-attacks reported in newspapers as headlines or in the news get everybody's attention which might make justifications easier, but when those fade, people's memory goes back to being difficult to justify doing these services and spending that money until something bad happens again.

Organization E considers that security is not very mature in the customer's mind in terms of something that is mandatory. It is not something that organizations do

as a luxury, organizations have to be vigilant and be as secure as possible all the time and there is where many of the customers are either naïve or they still struggle to build a security awareness mindset.

Organization E provides services to a very wide spectrum of customers which have different levels of security maturity. Some customers don't understand that information should be preserved and logged to be able do an investigation. Some others think that they just need to acquire some service when they need it and there will be all kind of vendors sitting there just waiting to be called, offering ample resources with no difficulties to provide help when needed. There are other more mature customers that acquire specific services to complement what they have within their organization and are on their way to build up internally the outsourced capability to be more self-sufficient.

Organization E highlights that customers are having a very difficult time attracting, finding and retaining skilled resources that can meet their growing demands and so are the providers. Finding dedicated people that do this work because this is what they love to do and they don't want to do other things, is hard. It is important to create bonds with universities and research groups. Moreover, this is a career path with high pressure and high burn-out. Skilled resources are on the road a lot, it is hard to have a life in this area and it is very stressful, because both the customers and the providers alike are looking over their shoulder constantly, both want answers and want them really fast. Furthermore, the skilled resources usually deal with unsophisticated customers, trying to translate things into an understandable dialogue that the customers can follow. There are a lot of frustrations and pressures in these roles. It is a very rewarding job to people that is not very stressful and can't get burned out.

> *"Security professionals are like doctors or surgeons who tell their clients precisely what they need to do to stay healthy and to cure themselves, but the clients ignore the advice and keep doing what they are doing. It is frustrating."*

5.5.2 Operation

Regarding Service Level Agreements, Organization E considers that there is no way to promise some customer that the provider's resources will be on site within a very specific amount of time. Everything is done of best effort and there are no artificial time limits. There is no way that a provider can promise to get to the bottom of something in an investigation in a certain period of time because each situation is different. It is hard to state service level agreements because there is no level of predictability in these kinds of situations.

> *"Sometimes the customer has the data available, sometimes they don't, and sometimes they have people that are available to work with the provider, but sometimes they don't."*

Organization E provides services often times to customers that can't afford to build up their own capability internally, because they think that security incidents happens rarely within their business and they don't need to have a dedicated group within their business to do this kind of work. However, when Organization E provides services to customers with an internal incident management team, the team is typically mature and self-sufficient. These customers are not looking to hire someone from the outside that command and assist them unless it is too complex; they are just too busy on other things going on within their business and need some support.

Organization E considers that when multiple providers are contracted to handle an incident, the customer is the one that dictates how the investigation should be done and defines the separation of duties to be handled by the companies that are brought in.

Organization E describes that the biggest difficulty in being able to perform incident response in real time is not being able to work remotely all the time. This is complicated, it might take a lot of bandwidth and a lot of customers don't like the idea of their data leaving the organization. If providers would be able to put agents on the customer's devices it would speed things up and make it much easier to get to the root cause of an incident. It will certainly speed up the information and would help to identify where did everything start.

Organization E considers that few customers are buying or consuming intelligence. Even though it is helpful to know if their organization is being targeted by any group, why they are targeting them, what kind of attack they would use in order to attack them and what are they after within their organization. Acquiring intelligence services will help the customers to look for the right kind of anomalies, the behaviour, the indicators of compromise, hopefully to be able to stop any attack from those groups.

Organization E believes that the biggest problem that the information security industry has is a too limited skill set. More efforts on producing the skills in a more adequate manner are required, so that they are not in such limited supply. Customers struggle, providers struggle and it is hard to do this work consistently because both customers and providers are fighting over a small number of resources that exist capable of doing this type of work. The need for these resources will keep growing, the more there is sophisticated technology such as cloud services, social networks and the internet of things, the more skilled and trained people will be required.

5.5.3 Post Operation

Organization E considers that there are no difficulties during the transition from one provider to another and describes that businesses that do this kind of work are quite professional and sophisticated so any provider is able to come in and follow up where the competitor left.

> *"I think the businesses that do this kind of work are pretty good and we are able to follow somebody else without much difficulty and I am sure that they are able to follow us if we don't keep doing the business. They are probably able to follow up on our work and do so pretty seamlessly."*

5.6 Case F

This section describes findings from Case F, where the interviewee has a security senior director role. Organization F is an enterprise-class Managed Security Service Provider.

5.6.1 Pre Operation

Organization F emphasizes that there are too many vendors in the market. From a customer perspective, it is very difficult to determine which of the managed security service providers, in the market around the world, are the right choice for the needs of the customers. All of them describe their services essentially in the same manner, but their products are in fact vastly differentiated. From a provider perspective, it is very difficult to convince the companies about how the provider's service solves the problem in a particular way and why the company should buy it from a specific provider. There are many other providers claiming to provide the same service and probably at a lower price but may not be doing it to a level of completeness. MSSPs should find the way to communicate their pro-activity, the skills and knowledge from their personnel and the methodology which their processes are aligned to.

Organization F describes that companies are concerned about passing a part of the business to a third party and the costs that this involves. Companies have to convince their decision makers that outsourcing the security services will provide an equivalence or improvement of capability. However, some companies are reluctant to buy services since outsourcing doesn't necessarily reduce security costs to the company but it tends to add new costs.

Organization F believes that customers should rethink the way they are looking for services in the market. They are looking at the technical specifications in many services not at the real challenges that they are trying to address. On the other hand,

MSSPs should better educate their customers on what they really do as a service provider and what they actually achieve inside their customers. MSSPs take the repeatable security tasks from the customers and bundles them to a standardized process. Then all those tasks get done all the time on schedule and in a predictable way.

Organization F outlines that security professionals, in small or medium size businesses, are responsible for a very large set of capabilities and as a result master few technology or are responsible for the implementation of all the technology. This leads to people setting the technology once and never revisiting it. People don't have the time, the energy or the capability to go back and keep constantly adjusting it to realign the technology to the constant changes in their environment and new threats in the cyber-world. The security personnel in those companies are in reality scattered over multiple technologies and don't have time to do things as a process. Whereas, the MSSP's personnel is constantly adjusting and changing what is needed. They face continuously some of the same problems with different customers and the knowledge acquired through similar cases is used to develop response processes.

Organization F highlights that companies are also concerned about losing job positions due to outsourcing. It is a real concern that produces animosity inside companies. The MSSPs need to persuade their customers that what they are doing is to take away the repeatable processes, so that the customer security personnel can do the interesting and new tasks. Instead of losing their jobs, the customer's personnel are benefited by improving their tasks. When their company outsourced security services, they get the opportunity to focus on the activities that actually demands high human skills opposed to the repeatable tasks.

Organization F emphasizes that MSSPs have staffing problems. They need to get sufficient people, skilled in sufficient technology to manage the customer needs. However, there is a shortage of skilled workers.

Organization F describes that many of the issues with managed security providers originate from the customer because the customers don't have good security control processes. The customers may have no control of their systems. They treat security as the last component of getting something done and because it is being outsourced, it is easier to blame the security provider instead of looking at the fact that they have inappropriate control of their own processes.

Organization F emphasizes that customers have to stop thinking that their security environment and security challenges are unique. They don't need to have something that is special to them.

"After many years of doing this, I have come across not a single customer that is in fact unique. Even though every single customer believes that is unique. However, you still have to say yes you are unique; we will place this just for you. In reality we don't, everyone in the industry knows this and unfortunately is beginning to play."

5.6.2 Operation

Organization F describes that in every single contract customers want changes from the standard process. Everyone wants something that is unique. The battle during the contract time is commonly on the control of the process, on the ongoing maintenance of the environment and on the support of the things agreed to support in the way that the customer wanted to be. Furthermore, something that also creates issues is the fact that customers don't know their environment.

MSSPs prefer to have control of the process because that allows them to keep the ability to keep a particular price for a commodity. The customer on the other hand, especially a new customer, doesn't want to give up the control that it has. Regarding the maintenance of the environment, it requires changes constantly and often times very rapidly. The problem is that in order to run the maintenance process correctly it has to match with how the customer runs their maintenance process on the rest of their environment. However, the rest of their environment is usually not aligned with good security practices. MSSPs need to negotiate with the customers about this topic especially at contract time.

Support to the customers can reach a huge level of complexity that is commonly not expressed at any point of time during the sales process because the customer omits details, or maybe is not aware of the complexity. In some cases, customers want specific versions of security technologies that may not be currently supported or they want their devices to be managed under a specific set of circumstances which are not industry standard but strange and unusual. Often times customers don't know what their environment is and the providers end up with all sorts of surprises during the contracting process. Customers may not understand what they are turning over to the provider so that the provider can actually take control of it.

Regarding roles and responsibilities, Organization F describes that MSSPs usually deal with two types of organizations: organizations with clear roles and responsibilities and organizations without clear designations. The ones with clear roles and responsibilities are usually those that are heavily regulated like the ones in the health care, financial or insurance industries. The ones without clear designations usually have shared responsibilities for specific roles and in some cases they even allow everyone the responsibility and the rights to make changes.

Organization F considers that penalties on a managed security service provider are an overload of requests to do things beyond how the provider sells the service. Customers will typically receive a certain amount of services provided on the contract for a given month. The provider will do some tasks constantly, and would be able to make a certain number of changes per month. Once the provider exceeds the number agreed in a given time period, the customer will start penalizing the provider because that is additional work that is not budgeted for the customer. The cost of this work will be charged back to the provider.

Organization F highlights that from the technical point of view, the reality of what leads to the current security confusion is that the development process is done in a customized manner. If everything would be done after a standard set of capabilities, the MSSPs could secure things much easier. The baseline would have a standard process and a standard way of addressing it. A good example for this is virtualization, in a virtualized environment all is in one place. MSSPs can apply security controls in a standardized manner.

Organization F describes that internal incident response teams benefit from additional workers in the process of incident response. For those customers that don't have an internal incident response team and have acquired the on-demand incident response capability, the providers end up running the incident response process for them or supporting them through the learning process as well as when they tumble around and figure out how to do it themselves.

Organization F believes that the MSS industry needs to focus on managing the capability not managing devices. The industry has only a small set of services to grow right now. It is important to find the way to make customers understand that what they need is not a set of services but a managed capability of security in their organization.

5.6.3 Post Operation

Organization F believes that customers are switching providers because they consider that they are paying too much for the service level that they get. As a consequence, they look for another MSSP that can offer them a better focus on them with more technical capabilities for a cheaper price. Another reason, but not so common, is when providers have made a mistake at some colossal scale and the trust with their customers is lost. Then, the customers leave the provider. However, in some cases providers get blamed for things that they can do nothing about.

Organization F highlights that in some cases customers are leaving the providers because they want to get back the services outsourced when they have matured. In

these cases, customers believe that they could do those services themselves much cheaper and much better.

Organization F describes that when a customer leaves a provider, the provider tries to transfer the customer's capabilities in a clean manner without any misses. This is always a challenge, especially considering that the provider is losing a costumer. The provider wants to give a good service, so that it can get the customer back at some point in the future. On the other hand, it is a loss and it is no longer the provider's responsibility. The provider might not want to put all the efforts into it if the new provider is not picking up doing everything as it should.

Organization F describes that customers are not very good at orchestrating the transition from one provider to another. The customer might want to control the process and make sure that the entire basis is covered. The customer might affect the transition if there are too many expectations. Furthermore, the customer doesn't hold the other vendor accountable for doing things as they should.

5.7 Case G

This section describes findings from Case G, where the interviewee is the manager of the threat intelligence and incident response team. Organization G is an emerging Managed Security Service Provider.

5.7.1 Pre Operation

Organization G describes that customers have difficulties to find out what they need. There is a gap between the technical people responsible for delivering security and the management board. The management board knows that there is a need to increase, in some way, the information security. Therefore the company looks for someone who can provide that service. As a consequence, there is often no link between the company needs and what the person responsible for acquiring the services is looking to protect. This person might not necessarily know what the business processes are and what is important for the company to protect. When providers try to find out what the company is trying to protect, it is often uncertain. There might be an idea of the systems and IT services that they would like to protect but in general there is no overview of the risk landscape that the company is facing.

Organization G helps its customers to look beyond finding services and discusses with the management board the actual needs. In some cases, a lightweight risk analysis is performed by risk and compliance consultants. Then, the results are transferred to the system environment level and presented to the management board as a tailored service that focuses on protecting the critical systems for the company.

With this approach Organization G closes the gap during pre-sales but also after a sale. It is an ongoing process to adapt the service to the company's needs to protect the critical assets in order to preserve the business.

5.7.2 Operation

Organization G highlights that there are different maturity security levels in companies and a varied level of ability to receive the service. It is not possible to deliver the same service at the same level to all different customers. The services require adapting and tailoring them to each one of the customers. Some of the customers are more mature and are able to consume the service in a more efficient and better way. They are able to get more value from the services provided. Organization G has also some customers that are not that mature. In these cases, it tries to help by educating them to become more mature and to receive the services provided by the organization more efficiently.

Organization G typically helps its customers with a low level of security maturity to build the ability to handle security incidents. It helps the customers by establishing a SOC or a CERT within the customer facilities. If the customers have the capability, the means and are willing to do it, Organization G helps them to establish an incident response framework, build tool sets and response exercises, build the entire incident response team and in some cases even the risk department. When the customers don't have enough resources or man-power, Organization G offers them consultants which could work as part of the customer team responsible for handling security incidents. The consultants will help the customers handling the incidents even without having a full incident response team and transferring knowledge to the employees of the customer's company. In a general approach customers get also workshops, training and help to build routines and procedures.

Organization G describes that when customers have an established incident response team, they hire certain services that are not efficient for them to have in-house, such as monitoring and analysis. In some cases, customers hire specific services or capabilities because are expensive to maintain such as forensic analysis or malware analysis. It is expensive to have these services in-house because companies can't really hire only one guy to do those things, they need a team working together, and that is hard to maintain in a smaller team.

One of the drawbacks of outsourcing is that customers don't necessarily build in-house the outsourced capabilities. They rely upon external parties to deliver all services and customers need to trust that the quality of what is being delivered is solid. Customers are dependent on the providers: if the provider is too busy to help a customer with a non-contracted service, the customer won't necessarily get the

needed help. The customers must pay for a premium service to have people standing by to react to emergency situations.

Organization G has multiple roles to ensure the quality of the different customer services that are delivered. There is usually a role in the customer organization which is the point of contact between Organization G and the customer. Organization G has a technical account manager responsible for the communication, a sales account manager responsible for the non-technical follow up on the customer and a range of roles that are common across multiple customers.

Organization G has a model for refunding monthly costs if penalties are incurred. Organization G's penalties are depending on the type of SLA broken, which have a percentage that is subtracted from the next month fee.

Organization G highlights that it has found a successful strategy to deal with the shortage of skilled personnel. Organization G uses external companies to receive candidates for interviews. However, in the latest years it has had success with hiring part time students that are doing a bachelor or master degrees in information security or in information technology. Organization G offers students a part time job and once the students graduate, it offers a job to those that are skilled and want to continue with their activities inside the organization.

> *"It has been a very successful strategy in terms of acquiring people. It is easier now after this initiative with students."*

Organization G describes that when multiple providers are involved in an incident each provider is typically hired to do specific tasks of the investigation. In some cases the eradication and recovery steps require to tune something that is not managed by the customer but by another provider. In these cases Organization G informs the customer and sends the specifications for modifications to the service provider in charge of that service. This approach might take some more time but it is working and helping more companies.

Organization G highlights that as long as security components involve humans, it can't do anything in real time. In order to work around this issue, customers need to give the service provider the ability to handle any incident 24/7 or customers need to build certain functions that runs 24/7 within their own company to be able to follow up on incidents 24/7. Customers are not reluctant to delegate management to MSSPs in terms of network access, network traffic, logs and system logs. However, some customers are reluctant to delegate management of end points to MSSPs. Organization G comments that decision makers need to be well informed about the

risks both in giving access to their MSSP and not doing it, because there are risks related to not handling incidents in a proper way.

Organization G describes that it sells dedicated intelligence services to a minority of its customers, only to those that are the most mature. Decision makers in the companies don't necessarily have abilities to define their own information needs. They don't know what threats are they facing, what decision they need to take and don't know what kind of information they need in order to make the right choices. They need help defining what information is needed. Only after the customer realizes what information is needed, can threat intelligence be provided.

Organization G emphasizes that some providers might offer threat intelligence services but in reality is just data feed. Data is not necessarily threat intelligence. Data must be evaluated and analysed to obtain consumable intelligence. Organization G gathers the data that will be used to obtain intelligence from multiple data sources such as partners, companies, individuals and through technical initiatives like multiple sensor networks.

Organization G considers that there are many MSSPs but little interaction among them. Something that would help the industry would be some kind of collaboration and information sharing in order to become better together.

5.7.3 Post Operation

Organization G describes that the few cases where it has lost customers it is because they wanted to have a global partner with global presence. Organization G has participated with best effort during the transition projects. In some cases, the new provider has not been able to handle something due to having no experience with certain equipment. Organization G has strict policies to not provide rule sets when passing equipment such as appliances. It will wipe the equipment and give the new provider a clean appliance. However, Organization G will have a full transition process when it is about operation centric services such as firewall operation, proxy operation and network operation services. It will send the new people, that have been hired to perform the same services, to India in order to educate and train them.

5.8 Expert 1

This section describes findings from Expert 1, where the interviewee is an independent security consultant with more than 15 years of industry experience managing and securing networks in both public and private sector. Expert 1 trains professionals on management of incident response teams.

5.8.1 Pre Operation

Expert 1 considers that the companies often times look for outsourcing as a lower cost alternative to maintaining on-site staff. Outsourcing provides the opportunity for lower cost services because it doesn't use dedicated staff. Service providers are able to offer companies a substantially reduced cost over having full time personnel on site all the time. The providers have people on staff that is looking at multiple different companies simultaneously. The positive side of this is that providers are in a position where they are able to see the occurrences across many different organizations, and take the expertise from each of those cases to convey that in terms of their capability in multiple customers. The negative side is that companies don't get the custom capability that internal staff functionality would have. It is very difficult for an outsource company to actually provide that level of capability and service.

Expert 1 describes that some companies don't really need a customized functionality. Some small and medium size businesses have very similar needs and providers know how to cover them effectively. The small companies look for a provider that can balance the cost functionality and is suitably for the functions that their businesses need. They usually just need somebody to pick up the telephone and call who is good enough to deal with the sort of problems that they have. However, some companies are "unique" and can't actually be compared to many other companies. These companies can't take advantage of all the outsourced capabilities needed to effectively run incident management for their company. They have tailor needs that require having internal dedicated staff with knowledge of the internal functionality of the business, nuances and specific requirements that their business has.

Expert 1 considers that small companies need to deal with knowing their own business, have a good established capability and report with the service provider and try to develop exercises for them to anticipate what could happen. They have to trust that the provider is acting in their best interest. On the other hand, large companies need to realize that the service provider is going to be essentially a partner providing expertise and then they need to find an organization that is committed to this capability for the long term. All companies need to be self-aware enough to understand how to transition all of the necessary information to the service provider.

Expert 1 recommends that when in doubt whether to outsource or not, companies should ask themselves if someone else can do the services better, faster and cheaper than them. If so outsource it. However, if it is something that involves data that the company should keep private and probably wouldn't want to allow out to any third party, then do not outsource that activity and improve it internally.

Expert 1 recommends building a contract protecting against problems associated with leaving that contract itself. An effective mechanism for identifying opportunities

to exit from a contract, if the contract is insufficient, is the concept of service level agreements. Both provider and customer agree to provide with functionality and to provide with money respectively, as long as the targets of performance are being met. When these targets are not met, then there is a vehicle by which the provider can attempt to amend the missed targets. If the targets continue to be missed then there is some other financial compensation and ultimately there is the opportunity for an early release from a contract because of missed targets.

5.8.2 Operation

Expert 1 highlights that companies with a partial outsourcing model might have internal expertise but don't have the time to actually develop some specific knowledge in-house or require a second opinion. Therefore, they look for a provider able to accomplish effectively whatever is necessary for that particular company.

Expert 1 describes that nowadays it is absolutely possible to have a fully outsourced model. It is possible to buy services for every single component that companies would need to have to run their incident management smoothly. Some companies just outsource all security services because that is not their core business; it is not how they make money. Then, instead of having staff trying to do security activities, they just look for experts on each one of those activities. Working with different partnerships essentially requires very clear contractual boundaries with each and every different partner involved. Therefore, companies should seek to minimize duplication of the same effort, clearly articulate what expect to receive for any particular component and what expect to return for any request. The difficulty, for any single company, is to manage the insertion points across different providers offering specialized services across different specialized topics. The alternative is to find some provider offering all these services but companies have to keep expertise within their organization in order to manage the interaction with the provider. Furthermore, the companies end up transferring a lot of control to the provider. The intellectual property concern is there across all companies, from small to large size companies.

Expert 1 typically recommends keeping expertise in-house. The in-house personnel are able to identify weak points of certain capability. They can encapsulate the components of those capabilities and identify boundaries where they could outsource the functionality of those components. Companies should use any outsource capability to make themselves substantially better. They should actively watch the outsourced functionalities and measure their effectiveness. Otherwise, they will be dumping money into something that will never really make the company better.

Expert 1 describes that the best model that he has seen is used by a company which is essentially entirely outsourced. The incident management functionality and all the technical functions were entirely outsourced. This is a large company based

on the United States with a global market share and an unquestioned market leader in what it does. This company has staffed people on the security department to manage the relationships with their various outsource partners. Whenever there has been an incident, the internal security staff knew who to address in the outsource company and all the capabilities that that company provides to them. The security staff manages all of the functionality but the functionality is all external.

Expert 1 recommends outsourcing services only when they will make the companies much more effective. Companies need to know what they need to accomplish internally and then obtaining the functionality externally. They should find the components that are absolutely most successful and find out what things within that successful component could be potentially outsourced. There might be things that were never done, or have been always done in the same manner, something might come up. This analysis on the successful components could develop an outsourcing capability. On the other hand, very small pieces within the components performing poorly should be outsourced. When something is performing poorly it is usually because the company doesn't understand what it should be doing. The company should think how it could more effectively perform this functionality and outsourcing is just one of the many opportunities to achieve improvement. Outsourcing that component often times doesn't teach the company what it should be doing. Furthermore, providers don't necessarily have the desire to improve the customer knowledge and they are comfortable with the fact that companies buying their services stay essentially ignorant to all the security functionalities that are necessary to do.

Expert 1 believes that a service provider should give an objective third party perspective identifying strengths and weaknesses to their customers. Providers should have a true intention of enhancing businesses and making those businesses more effective; even if that means that the providers train their customers to take some outsourced services back in house. From a partnership perspective, it ends up being a very powerful mechanism for improving everything for your customer. From a customer retention perspective, when the customers perceive that they are being helped to become better, they will not look for anybody else.

Expert 1 highlights that the incident response model of many companies is to wait for somebody to tell them that have been breached and then clean up. The latest data breach reports show that a high number of data breaches were not discovered by the company that was breached but were discovered by somebody else.

Expert 1 considers that real time response is an unapproachable accomplishment; it will generate too much noise. Instead of trying to detect everything in real time, companies should try to detect the things that really matter. Service providers and companies should focus on detecting systems once they have been compromised

within certain amount of time but aiming to not let the attackers get to their ultimate objective.

5.8.3 Post Operation

Expert 1 describes that companies need to make sure that they can always get their data back. Data and data in its many forms in terms of ownership and retention as well as the potential long term retrieval collection should be carefully defined in the contract.

Chapter 6
Discussion

In this chapter the findings from chapter 5 are discussed. Links are established between the findings and the research questions presented in section 1.1

6.1 How do outsourced incident management services benefit or affect current incident management teams?

Organization A describes that good communication with internal incident management teams depends on the customer's forensic readiness, meaning that the customer is prepared and the stakeholders are involved in the case. If there is not a proper working model in the internal incident management team, there might be communication conflicts due to a lack of internal communication.

A customer that has security controls in place, trains its people, has implemented security awareness and knows what might be the threats gets more benefit on the outsourced incident management services. Organizations E and G describe that when internal incident management teams are mature and self-sufficient, they look for assistance in services that are too complex or that are not efficient for them to have in-house. Organizations A and C explain that outsourced incident management services could benefit an internal incident management team by providing it with more man-power, specialized services, managerial skills, a global perspective on threats and multiple sources of intelligence. However, in some cases it might affect internal teams that are trying to respond in the same manner if there are not clear lines of responsibility in terms of which team does what type of tasks. Besides some internal incident management teams might get affected by a reduction of staff.

Organization B comments that current incident management teams benefit from participating in discussions and inputs coming from the provider getting a different perspective in order to make decisions and reach agreements to deal with an incident.

Organization D highlights that some internal incident management teams might

perceive the MSSPs as the help needed to prevent being fired when an incident is out of control. Therefore it is important to spend time with the internal incident management teams to understand better what is exactly needed from the provider to help them to be prepared for future incidents.

Organization F describes that internal incident response teams benefit from additional workers in the process of incident response. The internal incident team passes the repeatable processes to the provider and the team can focus now on tasks that demand human skills.

Organization F highlights that one of the drawbacks is that customers are dependent on the providers and won't build in-house the outsourced capabilities.

Expert 1 describes that internal incident management teams might be affected by outsourced services when the teams don't understand clearly what they should be doing. Outsourcing services won't teach them what to do and providers don't necessarily have the desire to improve their customer's knowledge. Some providers might be comfortable with the fact that their customers stay essentially ignorant to all the security functionalities that are necessary. However, internal incident management teams might benefit from outsourced capabilities that will provide them with better task performance on services that were already successful before contracting any service to the MSSP. As a result, successful security components are strengthened with outsourced services.

6.2 How are roles, responsibilities and penalties described in service level agreements between a customer and the outsourced incident management service's provider?

Organizations A and D describe that they offer different types of SLAs in terms of different services. Organization A's responsibilities and penalties are dependent on what the customer is looking for and is willing to pay. The penalties differentiate on what services are outsourced, traditional managed security services or managed incident handling services, the level of the incident missed and the severity of the attack.

Organization B explains that the roles and responsibilities are dependent on what the client wants, the higher the SLAs the more they have to pay because it requires more staff. Organization B offers different types of SLA's not only in terms of different services but also according to the environment (production, test, development, etc.). The SLAs related with the production environment have higher cost and penalties than the rest of the environments. The penalties at the SLAs might differ from account to account. However, Organization B has compensation agreements, meaning

that if an SLA is missed and there is a penalty, the compensation agreement could be used in order to condone the penalty as long as the compensation agreement is achieved.

Organization C has very specific SLAs for incident reporting or detection. If there is an incident or suspected incident, there is an escalation process to notify the customer, which is done by phone or by other means, based on its severity. But Organization C uses a different set of SLAs when it comes to incident response. Responsibilities and penalties are dependent on what is being offered and what the consequences are for the customer.

Organization E considers that there is no way to promise some customer that the provider's resources will be on site within a very specific amount of time. Everything is done of best effort and there are no artificial time limits. There is no way that a provider can promise to get to the bottom of something in an investigation in a certain period of time because each situation is different. It is hard to state SLAs because there is no level of predictability in these kinds of situations.

Organization F handles the penalties as an overload of requests to do things beyond how was agreed on the SLA. Once the provider exceeds the number of changes agreed in a given time period, the customer will start penalizing the organization because that is additional work that is not budgeted for the customer. The cost of this work will be charged back to Organization F.

Organization G has multiple roles to ensure the quality of the different customer services that are delivered. There is usually a role in the customer organization which is the point of contact between Organization G and the customer. There is a technical account manager responsible for the communication, a sales account manager responsible for the non-technical follow up on the customer and a range of roles that are common across multiple customers. Organization G's penalties are depending on the type of SLA broken, which have a percentage that is subtracted from the next month fee.

6.3 Which challenges are experienced during the implementation of these services in incident management?

6.3.1 Pre Operation

Customer's challenges

- **Identifying the services needed.** Many of the services are named differently

by different providers which makes it more difficult for non-security aware customers to find out the right services. Organization A recommends to make an in depth search of the services and then get an independent view from a third party, helping to understand what their strengths and weaknesses are and what might be suitable for the company. Organization C recommends that providers should be clear about where these services are located in the incident management process, where the starting point is, where the ending point is and what are the resources required from the customer in order to implement the services. Organization D, F and G recommend providers to devote time helping potential clients to understand how what they are doing is different from what others do and what some of the differences in their proposal are. Organization F advises the customers to not choose services through technical specifications but according to the real challenges that are trying to address. Expert 1 recommends outsourcing services only when they will make the companies much more effective instead of outsourcing services that are performing poorly. Companies need to know what they need to accomplish internally and then obtaining the functionality externally. They should find the components that are absolutely most successful and find out what things within that successful component could be potentially outsourced.

- **Choosing the right provider.** Companies are not aware of the broad diversity of providers that can offer them incident management services. Organization A advises the companies to have a subscription or a working relationship with an analyst company or a neutral third party in order to get an independent view of the providers, helping to understand the MSSP market segmentation, provider's capabilities, flexibility and customer satisfaction. Organization F recommends to find about the provider's pro-activity, the skills and knowledge from their personnel and the methodology which their processes are aligned to.

- **Taking into consideration the staff morale.** The staff morale might be affected by the decision of outsourcing services that were previously run in-house. In some cases the in-house personnel might be concerned about losing their job positions. Organization B recommends involving the staff, and making them understand why the decision was made and try to make it positive. Organization F advises MSSPs to persuade their customers that what they are doing is to take away the repeatable processes, so that the customer security personnel can do the interesting and new tasks. Instead of losing job positions, the in-house personnel would be benefited by improving its tasks.

- **Adapting to a foreign language communication when using global outsourced services.** Outsourcing services to global companies might impact the internal communication, since the staff might not be used to talking to

people in another language such as English. Organization B recommends taking the internal communication into account when choosing a service provider.

- **Predicting resources and justifying them inside the business.** Customers may have a very difficult time predicting how much resources or help they are going to need and justifying it within their business. Organization E advises to take advantage of cyber-attacks reported in newspapers as headlines or in the news to make justifications easier.

Provider's challenges

- **Having control over the outsourced service.** MSSPs prefer to have control of the process because that allows them the ability to keep a particular price for a commodity. The customers on the other hand, are reluctant to provide the control. Organization F recommends MSSPs to negotiate this with the customers especially at contract time because constant changes are required in a rapid manner and should be aligned to good security practices.

6.3.2 Operation

Customer's challenges

- **Communication between external and internal incident management teams.** Internal communication within an incident where clear roles and communication mechanisms have not been established in the internal incident management team can cause communication conflicts. Organization A describes that it is important that the customers have developed some forensic readiness and incident management planning describing IRT roles and responsibilities.
- **Multiple providers interaction during an incident.** Customers may have multiple providers supporting the same incident which, even if they are assigned to do different tasks, can have some overlap. Organization C recommends that there should be some hierarchy involved when multiple providers are engaged in the same incident, to make sure that somebody is in charge and perhaps solve overlapping tasks. Organization E describes that the customer should be the one dictating how the investigation would be done and defining the separation of duties to be handled by the companies that are brought in. Organization G recommends to inform the customer about overlaps and to be proactive and address the rest of the providers in charge of a specific security component overlapping, providing them with specifications for modifications. Expert 1 describes that working with different providers requires very clear contractual boundaries with each and every different partner involved. The

customers should seek to minimize duplication of effort, clearly articulating what is expected from each provider.

– **Collecting logs from systems and infrastructure.** Customers might not be logging what is happening in their infrastructure. The use of logs is something that does not necessarily require many resources, but it provides great help investigating an incident. Organization D advises to collect sufficient logs and data in order to facilitate and improve the customer's incident response process. This will allow verifying the information of an incident and would significantly speed the provider's response enabling some response functions to be performed remotely.

Provider's challenges

– **Providing emergency response services to new customers.** Emergency response services are those that companies can call on during 24 hours every day of the year when they have an emergency. Organization A advises that experienced security professionals which have developed their skills through different cases are the most suitable to provide help quickly in an unknown infrastructure, being fast and efficient on analyzing what happened, how can it be stopped and finding out what systems are in scope, in order to make the right choices for the response. Organization C describes that some customers prefer to engage multiple providers when emergency response services are required.

– **Having appropriate staff to provide response to emergency response calls.** MSSPs require having people available to respond when needed. Organization C advises that providers should be prepared to provide the appropriate people at the appropriate time, since their staff might be actively engaged in different tasks. Providers should have at least enough staff for those customers that have contracted services.

– **Reaching global support when system breaches involve global companies.** Some companies might have complex systems either in their internal infrastructure or due to the fusion with other companies. When there is a breach in global companies or in companies with complex systems, such as cloud services, it might demand to get the log files involved located in different countries. Organization A recommends not looking at the whole company, but first finding the breach and then working the way through it and through the systems. If there are complex systems involved in the breach, only then global resources might be required.

– **Combine the strategic information and the intelligence.** Not all vendors have access to the same multiple sources of intelligence or the knowledge

on what to do with it. Organization A describes that the quality of the input that you have access to as a vendor is a big differentiator, but then only by combining it with strategic information either from history or from experience, is when meaning can be extracted. Organization E advises that consuming intelligence will provide detection of the right kind of anomalies and indicators of compromise to stop targeted attacks.

- **Implementing massive security services that will work without false positives.** Many customers want to get security services alerting only about the real issues and not being alerted by stuff that is not relevant. Organization A describes that it depends on the quality of the services but this would achieved once a broader integration of IT, network and security systems occurs.

- **Keeping the customers.** Customers might switch providers due to not getting the agreed service or because the service is or becomes too expensive. Organization A describes that in order to keep a customer it is important to build a trusted relationship between the provider and the customer.

- **Cultural differences might impact the working behaviour.** Offshoring is the relocation of an outsourced service from one country to another that provides cheaper labor costs. The cultural differences in those outsourcing destinations might impact the communication and the working behaviour in the provider's staff. Organization B explains that having workers with big cultural differences demands follow up activities and inter-cultural communication in order to understand the differences and get the job done.

- **Unavailable offshore personnel working in countries with natural, societal or political risk factors.** Different circumstances such as natural disasters, strikes or riots among others might restrict offshore workers to reach their working place. Organization B describes that having offshore offices spread over different locations is a good way to spread the risk and not have an impact on the offshore services provided.

- **Remote response enabled by agents.** Customer's IT departments might be reluctant to use agents because for every incremental bit of complexity on an endpoint there is potentially a large percentage of customer service calls, help desk calls, and an increase in the time of evaluating new software or operating system releases. Organization D and E recommend working with customers to help convincing their ultimate decision maker as to why the benefit of running the agent at the endpoint is greater than the cost.

- **Lack of skilled personnel.** Shortage of people with capabilities for incident response activities. It is difficult to hire as many people as is needed. Organization D advises to hire more junior talent to develop their skills providing them

with formal training and in-depth hands-on experience. Organization E advises to create bonds with universities and research groups to find dedicated people and train them. Organization G recommends offering students a part time job while they write their thesis. Once the students graduate, organizations can select those that are skilled and want to keep inside by offering a full time job position.

- **Incident response roles are not clearly defined.** Incident response roles are not clearly defined in the industry, when hiring incident response experts there is a wide variation of the capabilities, level of experience and expertise that is needed. Organization D recommends defining internally what these roles actually are for the company's needs. It is important to understand, when hiring new personnel, what they really have experience in and how that is related to what it is needed at any particular point.
- **Different security maturity levels.** Customers have different levels of ability to receive the managed security services. Organization G tries to help its costumers, with a low level of maturity, by educating them in order to receive its services more efficiently. It helps these customers to establish a SOC or a CERT and offers them consultants which could work as part of the customer team responsible for handling security incidents. For those customers with better capabilities and more mature level of security, it helps them to establish an incident response framework and to build tool sets and response exercises.

6.3.3 Post Operation

Customer's challenges

- **Knowledge transition of customer services from one provider to another when a customer changes provider.** Providers might be reluctant to pass knowledge that took many years to get. Some of this knowledge might not be documented and does not reach the new provider. Organization B describes that providers might transition the problem knowledge that they are obliged to but not the rest. Having proper documentation and a continuous revision of it during the meetings with the customer might help to keep everything documented so that there won't be any gaps when a provider transition will occur. Organization D highlights that the new provider should be aware that the previous provider may not have much incentive to participate on the process since they are losing a contract. Organization G emphasizes that in some cases it is needed to educate and train the new people that have been hired to perform the same services.

Provider's challenges

– **Understanding the customer needs and expectations when switching providers.** Not understanding the new customer's expectations and its infrastructure could make the transition challenging for the provider receiving the new costumer and deteriorate the relationship from the beginning. Organization A emphasizes the importance of getting familiar with the infrastructure both at the customer and previous provider's facilities. It is important to understand what the critical assets are, what does the customer wants to protect and where the previous provider failed. The more the provider knows about the customer then the better it would be in shape to provide protection and build a trusted relationship between the parties. Organization C describes that the provider needs to understand the new customer's challenges in order to identify the services that can be offered in that category and propose something to address them based on their prior experience.

6.4 What are the future needs for outsourced incident management and what is lacking from the industry to make it real?

Organization A highlights the importance of keeping up with the technology, the misuses of it and being aware of the trends and prices on the dark market. Everyone needs to be more prepared because those that are misusing the technology are continuously looking for new vectors of attack.

Organization A emphasizes the need to change the classical computer forensics into a process that includes identifying, preserving, recovering and analysing evidence from big data, cloud services and multiple hosts. The industry needs to evolve the current digital investigations methodology.

Organization A describes that customers want many security services implemented working without false positives. The industry needs to better integrate IT, network and security systems.

Organization A recommends to continue contributing on building security awareness and knowledge, there are still a lot of people thinking that they don't have any data that someone would be interested in getting. There are some others that are spending money on services that provide them with more vision on what is happening but don't know what to do with that data.

Organization B highlights the importance of inter-cultural communication to achieve better quality global services.

Organization C outlines that the industry is still lacking better automation and

better integration to address incidents. More integration of multiple incident response tools is needed to offer more complete software packages, as well as integration from software vendor's products and MSSP's tools. Threat data and threat intelligence needs to be better integrated with the tools used for incident handling.

Organization D recommends to switch from the linear NIST incident response model to a loop concept such as the OODA loop (Section 3.8) to change the efficiency and effectiveness of processes.

Organization E highlights that the limited supply of skilled personnel needs to be addressed and the industry should collaborate more effectively with universities to produce talented people.

Organization F describes that the MSS industry needs to transition from managing devices to managing the security capability in their customers. MSSPs need to find the way to make customers understand that what they need is not a set of services but a managed capability of security in their organization.

Organization G emphasizes that decision makers in the companies don't have necessarily abilities to define their own information needs regarding threat intelligence. They don't know what threats are they facing, what decisions they need to take and don't know what kind of information they need in order to make the right choices. Customers need to be aware that some MSSPs might offer threat intelligence services but in reality is just data feed.

Organization G considers that collaboration and information sharing among MSSPs would benefit the industry.

Expert 1 recommends that instead of trying to detect everything in real time, the focus should be on trying to detect the things that really matter. Service providers and companies should focus on detecting systems once they have been compromised within a certain amount of time but aiming to not let the attackers get to their ultimate objective. Organization G highlights that as long as security components involve humans, it can't do anything in real time. It recommends companies to give the service provider the ability to handle functions to follow up on incidents 24/7 or to build functions in-house with the capabilities to do a follow up on incidents 24/7.

Expert 1 believes that providers should have a true intention of enhancing businesses and making their customer's businesses more effective; even if that means that the providers train their customers to take some outsourced services back in house.

Chapter 7
Conclusion

Six large managed security service providers (MSSPs) and one emerging MSSP were studied. These providers were selected based on their leadership in the marketplace, their suite of IT outsourcing and business process outsourcing security services and staff dedication to managed security services. Furthermore, an independent expert provided insights and recommendations on current practices performing incident management through outsourced services. The independent expert was selected based on his knowledge and experience as independent security consultant as well as his experience training on management of incident response teams.

The interviewees have different roles in their respective organizations, this provided a broader perspective on the challenges including the technical and the business perspective. The customer and provider's challenges described in Section 6.3 were both described by the interviewees. However, none of the interviewees is part of a client organization. This provides a unilateral perspective on the challenges. Moreover, only two out of the three categories of MSSPs were interviewed.

7.1 Summary

The interviews revealed some of the challenges that outsourcing incident management services are currently posing to both customers and providers. Those that can be highlighted are: identifying the services needed, multiple providers interaction during an incident, lack of skilled personnel and knowledge transition of customer services from one provider to another when a customer changes provider.

Most of interviewees outline the lack of agreement on the nature of the services. A categorization and summary of the current incident management services offered by the most significant providers in the market was created and presented in section 3.6. The interviewees recommend to evaluate the quality of the services through a neutral third party.

Most of the interviewees agree on benefits and disadvantages to existing internal incident management teams when the partially outsourced model is taken. Some of the benefits mentioned are: more man-power, specialized services, managerial skills, a global perspective on threats and multiple sources of intelligence. Some of the disadvantages are: overlaps when there are not clear lines of responsibility, reduction of staff.

Most of the interviewees described different ways of handling penalties in SLAs. Penalties can be dependent on the service outsourced, the environment (production, test, development), the level of the incident missed, the severity of the attack, and the consequences for the customer. Moreover, penalties can be charged for exceeding the number of changes agreed in a given time period, which is consider additional work that is not budgeted for the customer.

Outsourcing incident management security services is an adequate option to get competent security for today's threats. Outsourcing incident management services might be a good option for small and medium size organizations that don't require any unique capabilities. These organizations are benefiting from affordable comprehensive security without investing in new infrastructure or being burdened by deployment and management costs.

Large organizations are benefiting by specialized services or by having the chance to focus on tasks that demand specialized skills instead of repeatable tasks. Tailored solutions are not easily achieved by outsourced services. It is a complex process that requires both internal and external staff to accomplish.

A fully outsourced model complemented with internal security experts is described by Expert 1 as a successful model for outsourcing incident management services. In this model, in-house security experts would manage the relationships with the various providers. The internal staff would know who to address in the outsource company and all the capabilities that the provider offers to them. The security staff manages all of the functionality but the functionality is all external.

Many of the emerging managed security service providers have been acquired by bigger companies, not necessarily bigger MSSPs. Ferrara [FMC14] outlines that the MSSP market has a solid and stable growth. The MSSP market might be attractive for traditional advisory service consultancies for reasons such as a broader client base, annuity based contracts and predictable capital that quality MSSPs typically enjoy. On the other hand, big MSSPs are looking to expand their growth and market leadership across the globe. This will lead to new acquisitions.

The MSSP market is also becoming a bazaar of services resold by various providers. Customers need to know which services are being resold to them and prevent clauses

in the contractual agreements where the provider does not guarantee the security of the client data when a service from a third party is resold.

The largest MSSPs (enterprise-class) have operations in multiple geographic locations, commonly in key high-tech locations in low-cost countries. When choosing the right provider it is important to consider the risks that the operation in those countries could face as well as how cultural differences can impact the business offshoring the services. Siepmann [Sie13] describes some of the aspects that should be considered: society, political stability, economy, crime, environment and infrastructure.

Communicating accurate threat information at a rapid pace will reduce information security risks. Collaboration from the public and private sector, including MSSPs, sharing threat intelligence will benefit everyone in gaining advance notice about cyber-attacks. Security incident characteristics can be formally described in a structured manner and shared through numerous security data-sharing options. Kampanakis [Kam14] summarizes the most prevalent information sharing models such as Trusted Automated Exchange of Indicator Information (TAXII), Cyber Observable Expression (CybOX), Structured Threat Information Expression (STIX), Real-Time Inter-network Defense (RID) and others.

The fundamental building blocks that are used to build technology today don't provide the capability of being resilient. More fundamental changes in today's technologies are required in order to reach resiliency. Integration with threat intelligence needs further development. Furthermore, combining threat intelligence with either the decision making OODA' cycle or the kill chain life cycle could benefit the defender's incident handling tasks and improve the holistic situational awareness with a threat-based active defense.

Hutchins et al. [HCA11] depicts how mapping security controls and procedures to each stage of the intrusion kill chain model could help developing very detailed, result-oriented security procedures. Schneier [Sch14] outlines that pulling different services together under a unified framework like the the Observe, Orient, Decide, Act (OODA) loop will make incident response work. In a similar manner mapping the outsourced incident management services to the incident management model presented in section 3.3 will facilitate the customers finding their needs, and will provide them with better understanding of what they are lacking to increase the effectiveness of their organization's cyber-defense capabilities.

The threat landscape is evolving, and new environments such as mobile, cloud, Internet of Things (IoT) and Machine to Machine (M2M) are introducing new challenges. This means that the lack of enough skilled security professionals will remain a problem also in years to come. Adequate training strategies are required to reduce the global cybersecurity skills gap. Building a security-minded culture

will prevent many successful and easily preventable attacks and a security-minded culture that's dedicated to constant improvement will improve the cyber-security personnel skills and attract new talent.

7.2 Further work

Knowledge transition of customer services from one provider to another requires proper documentation. This documentation is not effectively managed, according to some of the interviewees, and in some cases there is knowledge that doesn't reach the new provider. Therefore exchange formats between providers to transfer the customer services knowledge could help to guarantee the customers that their data will be properly handled during and after the transition. A public file format for exchange of customer services knowledge should be developed to automate as much of the knowledge transition process as possible. It would make cross-organizational coordination more efficient and cost effective.

Better visibility of the whole incident management in-house through dashboards might provide new ways to discuss and share information with everyone involved in the incident management team, e.g., public affairs office, legal department, management; in order to increase effectiveness of the organization incident handling process.

References

[ADK+04] Chris Alberts, Audrey Dorofee, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. Defining incident management processes for csirts: A work in progress. Technical report, DTIC Document, 2004.

[AGM+03] Julia Allen, Derek Gabbard, Christopher May, Eric Hayes, and Carol Sledge. Outsourcing managed security services. Technical report, DTIC Document, 2003.

[AJ14] Massimiliano Albanese and Sushil Jajodia. Formation of awareness. In *Cyber Defense and Situational Awareness*, pages 47–62. Springer, 2014.

[BBC06] W Brotby, J Bayuk, and C Coleman. Information security governance: guidance for boards of directors and executive management, 2006.

[BDD+10] Paul Barford, Marc Dacier, Thomas G Dietterich, Matt Fredrikson, Jon Giffin, Sushil Jajodia, Somesh Jha, Jason Li, Peng Liu, Peng Ning, et al. Cyber sa: Situational awareness for cyber defense. In *Cyber Situational Awareness*, pages 3–13. Springer, 2010.

[Boy87] John R Boyd. Organic design for command and control. *A discourse on winning and losing*, 1987.

[Bri07] British Standards Institution. BIP 0107:2008 foundations of IT service management based on Itil V3. Standard, British Standards Institution (BSI), UK, 2007.

[CMGS12] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone. Computer security incident handling guide. *NIST Special Publication*, 800:61, 2012.

[Des05] Deepali Deshpande. Managed security services: an emerging solution to security. In *Proceedings of the 2nd annual conference on Information security curriculum development*, pages 107–111. ACM, 2005.

[DYY05] Wen Ding, William Yurcik, and Xiaoxin Yin. Outsourcing internet security: Economic analysis of incentives for managed security service providers. In *Internet and Network Economics*, pages 947–958. Springer, 2005.

[End88] Mica R Endsley. Design and evaluation for situation awareness enhancement. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 32, pages 97–101. SAGE Publications, 1988.

[FH13] Ed Ferrara and Nick Hayes. The forrester wave: Emerging managed security service providers, q1, 2013. *Forrester Research, January*, 2013.

[FMC14] Ed Ferrara, Christopher McClean, and Michael Caputo. The forrester wave: Managed security services: North america, q4, 2014. *Forrester Research, November*, 2014.

[GTK+10] Michael N Gagnon, John Truelove, Apu Kapadia, Joshua Haines, and Orton Huang. Towards net-centric cyber survivability for ballistic missile defense. In *Architecting Critical Systems*, pages 125–141. Springer, 2010.

[HBL10] Sharlene Nagy Hesse-Biber and Patricia Leavy. *The practice of qualitative research.* Sage, 2010.

[HCA11] Eric M Hutchins, Michael J Cloppert, and Rohan M Amin. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1:80, 2011.

[ISO11] ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management. Standard, International Organization for Standardization (ISO), Geneva, CH, September 2011.

[ISO13a] ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements Preview. Standard, International Organization for Standardization (ISO), Geneva, CH, November 2013.

[ISO13b] ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls. Standard, International Organization for Standardization (ISO), Geneva, CH, October 2013.

[JNK+11] Sushil Jajodia, Steven Noel, Pramod Kalapa, Massimiliano Albanese, and John Williams. Cauldron mission-centric cyber situational awareness with defense in depth. In *MILITARY COMMUNICATIONS CONFERENCE, 2011-MILCOM 2011*, pages 1339–1344. IEEE, 2011.

[Kam14] Panos Kampanakis. Security automation and threat information-sharing options. *Security & Privacy, IEEE*, 12(5):42–51, 2014.

[KKRZ05] Georgia Killcrece, K Kossakowski, R Ruefle, and M Zajicek. Incident management. *Build Security In*, 2005.

[KTM11] Gabriel Klein, J Tolle, and Peter Martini. From detection to reaction-a holistic approach to cyber defense. In *Defense Science Research Conference and Expo (DSR), 2011*, pages 1–4. IEEE, 2011.

[Mer14] Sharan B Merriam. *Qualitative research: A guide to design and implementation.* John Wiley & Sons, 2014.

[MN07] Michael D Myers and Michael Newman. The qualitative interview in is research: Examining the craft. *Information and organization*, 17(1):2–26, 2007.

[MRS10] Miroslav Maj, Roeland Reijers, and Don Stikvoort. Good practice guide for incident management, 2010.

[Rey14] Alfredo Reyes. Incident Management in Outsourcing. Project report (minor thesis), NTNU, 2014.

[Rob11] Colin Robson. *Real world research: a resource for users of social research methods in applied settings.* Wiley Chichester, 2011.

[Sch02] Bruce Schneier. The case for outsourcing security. *Computer*, 35(4):0020–21, 2002.

[Sch14] Bruce Schneier. The future of incident response. *Security & Privacy, IEEE*, 12(5):96–96, 2014.

[She97] John Sherwood. Managing security for outsourcing contracts. *Computers & Security*, 16(7):603–609, 1997.

[Sie13] Frank Siepmann. *Managing risk and security in outsourcing IT services: Onshore, offshore and the cloud.* CRC Press, 2013.

[Tho06] David R Thomas. A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation*, 27(2):237–246, 2006.

[TLJ14] Inger Anne Tøndel, Maria B Line, and Martin Gilje Jaatun. Information security incident management: Current practice as reported in the literature. *Computers & Security*, 45:42–57, 2014.

[Wen01] Tom Wengraf. *Qualitative research interviewing: Biographic narrative and semi-structured methods.* Sage, 2001.

[Yin13] Robert K Yin. *Case study research: Design and methods.* Sage publications, 2013.

[ZXW09] Xia Zhao, Ling Xue, and Andrew B Whinston. Managing interdependent information security risks: A study of cyberinsurance, managed security service and risk pooling. *ICIS 2009 Proceedings*, page 49, 2009.

Appendix

A Request for participation in research project

This section includes the request for participation in research project provided to the case study participants. This request describes the background and purpose of the research, briefs the participants about the implications of their participation and how their information will be treated.

This document is a consent form reported to the Norwegian Social Science Data services.

Request for participation in research project "Outsourced Incident Management"

Background and Purpose
Nowadays attacks, security environments and organizations have changed due to outsourced settings. Therefore new products and services for response are reacting differently. Some companies provide outsourced monitoring and management of security devices and systems. Outsourcing the incident management seems to be a cost-effective way to satisfy some small and large organization's requirements.

Outsourcing the incident management comes with a set of challenges. This topic is currently not well-explored by researchers, hence further investigations are needed to identify whether there are specific challenges on relying on outsourced services for incident management, such as prevention, detection and response.

The project is a Master's thesis at the NTNU that aims to explore this topic. The sample has been selected according to the kind of services outsourced/provided.

What does participation in the project imply?
Data will be collected through interviews, the questions will concern: incident management, outsourced security services, roles, responsibilities, penalties, challenges. The data collected will be collected in audio recordings.

What will happen to the information about you?
All personal data will be treated confidentially. Personal data will be accessed only by the student and supervisors. Personal data/recordings will be stored as encrypted files to ensure confidentiality. Participants will not be recognizable in the publication.

The project is scheduled for completion by 31st May 2015. At that point, personal data and any recordings will be securely erased.

Voluntary participation
It is voluntary to participate in the project, and you can at any time choose to withdraw your consent without stating any reason. If you decide to withdraw, all your personal data will be made anonymous. If you have any questions concerning the project, please contact:

Alfredo Reyes (Student)	alfredor@stud.ntnu.no	+47-944 30 063
Martin G. Jaatun (Supervisor)	martin.g.jaatun@sintef.no	+47-900 26 921
Colin Boyd (Supervisor)	colin.boyd@item.ntnu.no	+47-735 51 758

The study has been notified to the Data Protection Official for Research, Norwegian Social Science Data Services.

Consent for participation in the study
I have received information about the project and am willing to participate

---
(Signed by participant, date)

Figure A.1: Request for participation in research project provided to the case study participants

Appendix B
Interview guide

This section presents the interview guide used as a sketch during the remote interviews.

The questionnaire guide during the interviews did not follow any predefined order to promote a fluent conversation. Elaborations where asked for when needed.

Outsourced Incident Management Alfredo Reyes

Interview guide

1. What is (are) your role(s) in the organization/company/?
2. What is your experience with outsourced incident management services?
3. What are the challenges that organizations are experiencing with outsourced incident management services?
    a. Why do these challenges arise?
    b. What can be done to address the challenges?
4. How do outsourced incident management services benefit or affect current incident management teams?
5. How are roles, responsibilities and penalties described in service level agreements between a customer and the outsourced incident management service's provider?
6. What is lacking from the industry to address the future needs?

Figure B.1: Questionnaire guide used during the remote interviews

Appendix C

Notification to the Norwegian Social Science Data Services

This section includes the notification receipt provided by the Norwegian Social Science Data Services. This receipt describes the estimated end date of the project and how the data collected would be made anonymous.

Norsk samfunnsvitenskapelig datatjeneste AS
NORWEGIAN SOCIAL SCIENCE DATA SERVICES

Harald Hårfagres gate 29
N-5007 Bergen
Norway
Tel: +47-55 58 21 17
Fax: +47-55 58 96 50
nsd@nsd.uib.no
www.nsd.uib.no
Org.nr. 985 321 884

Colin Alexander Boyd
Institutt for telematikk NTNU

7491 TRONDHEIM

Vår dato: 20.02.2015 Vår ref: 42023 / 4 / HIT Deres dato: Deres ref:

TILBAKEMELDING PÅ MELDING OM BEHANDLING AV PERSONOPPLYSNINGER

Vi viser til melding om behandling av personopplysninger, mottatt 03.02.2015. Meldingen gjelder prosjektet:

42023	*Outsourced Incident Management*
Behandlingsansvarlig	*NTNU, ved institusjonens øverste leder*
Daglig ansvarlig	*Colin Alexander Boyd*
Student	*Alfredo Reyes*

Personvernombudet har vurdert prosjektet og finner at behandlingen av personopplysninger er meldepliktig i henhold til personopplysningsloven § 31. Behandlingen tilfredsstiller kravene i personopplysningsloven.

Personvernombudets vurdering forutsetter at prosjektet gjennomføres i tråd med opplysningene gitt i meldeskjemaet, korrespondanse med ombudet, ombudets kommentarer samt personopplysningsloven og helseregisterloven med forskrifter. Behandlingen av personopplysninger kan settes i gang.

Det gjøres oppmerksom på at det skal gis ny melding dersom behandlingen endres i forhold til de opplysninger som ligger til grunn for personvernombudets vurdering. Endringsmeldinger gis via et eget skjema, http://www.nsd.uib.no/personvern/meldeplikt/skjema.html. Det skal også gis melding etter tre år dersom prosjektet fortsatt pågår. Meldinger skal skje skriftlig til ombudet.

Personvernombudet har lagt ut opplysninger om prosjektet i en offentlig database, http://pvo.nsd.no/prosjekt.

Personvernombudet vil ved prosjektets avslutning, 31.05.2015, rette en henvendelse angående status for behandlingen av personopplysninger.

Vennlig hilsen

Katrine Utaaker Segadal

Hildur Thorarensen

Kontaktperson: Hildur Thorarensen tlf: 55 58 26 54
Vedlegg: Prosjektvurdering

Dokumentet er elektronisk produsert og godkjent ved NSDs rutiner for elektronisk godkjenning.

Figure C.1: Notification receipt provided by the Norwegian Social Science Data Services

Personvernombudet for forskning

Prosjektvurdering - Kommentar

Prosjektnr: 42023

The sample will receive written information about the project, and give their consent to participate. The letter of information is well formulated.

The Data Protection Official presupposes that the researcher follows internal routines of NTNU regarding data security. If personal data is to be stored on portable storage devices, the information should be adequately encrypted.

Estimated end date of the project is 31.05.2015. According to the notification form all collected data will be made anonymous by this date. Making the data anonymous entails processing it in such a way that no individuals can be recognised. This is done by:
- deleting all direct personal data (such as names/lists of reference numbers)
- deleting/rewriting indirectly identifiable data (i.e. an identifying combination of background variables, such as residence/work place, age and gender)
- deleting audio recordings

Figure C.2: Notification receipt provided by the Norwegian Social Science Data Services (Continued)

Appendix D

Paper under review for CloudCom 2015 conference

This section includes the paper submitted to the 7th IEEE international conference on cloud computing technology and science (CloudCom).

Passing the Buck: Outsourcing Incident Response Management

Alfredo Ramiro Reyes Zúñiga* and Martin Gilje Jaatun†
* Department of Telematics, NTNU, Trondheim, Norway
†SINTEF ICT, Trondheim, Norway

***Abstract*—Many organisations are outsourcing computer operations to third parties, and the next logical step is to outsource management of computer security incidents as well. This paper describes a case study where we have studied several organisations who are active in this space today. Our results indicate that outsourcing of incident management is a viable security approach for many organisations, but that transitioning between providers frequently is a challenge.**

***Index Terms*—Outsourcing; incident response; security**

I. Introduction

Today's evolving Information and Communication Technology (ICT) environment requires connecting not only new applications and devices, but also new providers and partners. As a result the ICT environment has been gradually outsourced to third parties, expanding the security perimeter. Some organizations are moving their ICT infrastructure to the cloud, where the options for incident response are either null or depending on third parties, with legal and accountability issues. Moreover, attackers (motivated, skilled and well-funded) are discovering new attack vectors, while defenders have to take care of multiple technologies and keeping them and themselves updated.

Incidents will occur sooner or later, but the important thing is to detect, contain and eradicate the incident quickly and effectively to reduce the impact to the organization. However, organizations under-invest on prevention and suffer from scarcity of skilled personnel. An evolving threat landscape and the lack of expertise in many organizations require new strategies to balance the need to manage incidents effectively.

Some companies provide outsourced monitoring and management of security devices and systems. Outsourcing incident management services seems to be a cost-effective way to satisfy some organizations' requirements. These kinds of providers are able to see a big picture view, by using the knowledge acquired by their solutions as their advantage.

A. Participants

The participant organizations is this study are transnational organizations selected based on the managed security service provider's (MSSP) market presence. Five large MSSPs contributed to the interviews.

B. Paper Structure

The remainder of this paper is structured as follows: We present related work in Section II, and elaborate on relevant standards in Section III. We provide more background on incident management in Section IV, and present our results in Section V. Section VI concludes the paper.

II. Related Work

The term incident management refers to the actions and mechanisms used to manage information security incidents. It is used to describe the collection of tasks involved with the incident response life-cycle. These tasks include plan and prepare for, detection and reporting, assessment and decision, responses, and lessons learnt to prevent future incidents.

Different standards, guidelines and frameworks have direct and indirect remarks on incident management. Those that are most notable among the information security community are: NIST SP 800-61 [1], ISO/IEC 27035 [2], ENISA Good Practice Guide for Incident Management [3] and ITIL [4]. These standards, guidelines and frameworks will be described in Section III.

Siepmann [5] describes outsourcing as contracting out services, previously performed internally, to a third party. Both the third party and the organization contracting out the services take part in a contractual agreement that involves payments, and exchange of services.

A great amount of academic literature related to incident management and managed security services (MSS) has been published. Nevertheless, the literature focused on outsourced incident management services is scarce. Siepmann [5] presents an analysis on security and privacy impacts when outsourcing Information Technology (IT) processes as well as recommendations on outsourcing preparation. Sherwood [6] studied the concerns regarding security of information within outsourced settings. The study presents a strategy to manage information security on outsourced technical services.

The study performed by Tøndel et al. [7] on current practices and experiences with incident management, identified the practice of incident management in outsourcing scenarios as one of the challenges for incident management. In accordance with their study, there is a need for improved understanding of the challenges of incident response in outsourcing scenarios particularly when several suppliers are serving the same customer.

Maj et al. [3] discuss the outsourcing of incident manage-

ment from the Computer Emergency Response Team (CERT[1]) point of view. They suggest hiring the right people to guide the outsourcing process since it is a challenging project that should not be underestimated. Maj et al. recommend keeping control over the incident handling services and not outsource those elements of incident handling that provide control such as incident reports, registration, triage (including verification and classification) and the overall coordination of incident resolution. Some of the reasons given to outsource incident management related services are [3], [8] :

- Cost.
- Difficulties in hiring, training and retaining staff.
- Services you might not want to provide yourself.
- Physically hardened facilities with latest infrastructure.
- Enterprise-wide management of security strategy.
- Access to threat and countermeasure information.
- Global prosecution.
- Service performance 24x7.

There is a need for research on the topic of outsourced incident management services since related information is scarce [9]. Siepmann's work [5] addresses management of information security incidents but his comments are only considered on managing incidents in outsourcing settings and not managed by a trusted third party outsourcing the services. Sherwood's study on management of security on outsourcing contracts [6], does not have an assessment on incident management. Tøndel et al.'s study on current practices and experiences with incident management [7] does not describe any outsourced incident management experiences or practices. The good practice guide for incident management published by Maj et al. [3] only addresses outsourcing of incident management from the CERT's perspective.

III. Standards and guidelines

This section introduces some standards containing information regarding incident management.

A. NIST Special Publication 800-61

This standard [1] aims to assist organizations in mitigating risks from computer security incidents by providing guidance on establishing incident response capabilities. It includes guidelines on building incident management capabilities and the interaction with external parties, such as vendors or Computer Security Incident Response Team (CSIRT).

NIST SP 800-61 describes in detail the four major phases of the incident response life cycle. These phases are (see Fig. **??**):

- Preparation.
- Detection and Analysis.
- Containment, Eradication and Recovery.
- Post-Incident Activity.

B. ISO/IEC 27035:2011 Information security incident management

This standard [2] provides guidance to incident management. It offers a structured approach to deal with incidents including planning, detecting, responding and thereafter extracting lessons learnt. ISO/IEC 27035:2011 presents five phases with recommended activities. These phases are:

- Plan and Prepare.
- Detection and Reporting.
- Assessment and Detection.
- Responses.
- Lessons learnt.

ISO 27035 aims to assist organizations in satisfying the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS) specified in ISO/IEC 27001:2013 [10]. ISO 27035 provides guidelines on the implementation of good practices on information security management presented in the standard ISO/IEC 27002:2013 [11].

C. ENISA - Good Practice Guide for Incident Management

ENISAs guide [3] provides guidelines for security incident management. It provides recommendations on the creation of a CERT and assists on preparing its mission, constituency, responsibility, mandate organizational framework and the type of services, in terms of the incident management process, that can deliver.

This guide highlights the incident handling process, and provides related information on roles, workflows and policies. ENISA's guide pays no attention to the preparation phase and focuses on the incident handling process composed by four phases: detection, triage, analysis and incident response.

D. The ITIL Framework

The ITIL framework [4] is a source of good practice for service management that focuses on aligning IT services with the needs of the organization. The main goals of the incident management lifecycle are to reestablish a normal service as fast as possible and to reduce unfavorable impact on business operations. During the incident management process, resources are assigned to different activities such as identification, registration, categorization, prioritization, diagnosis, escalation, investigation, resolution, recovery, and incident closure, in order to mitigate and minimize the impact of incidents. The incident management process can be triggered by incident reports coming from diverse sources.

IV. Incident management

There is a lack of consistency in defining incident management across the standards and guidelines as well as in the information security literature. The terms incident management, incident handling and incident response are in some cases used interchangeably. However, these terms have a different scope.

[1]The term CERT was used for the first time by the Computer Emergency Response Team Coordination Center (CERT-CC) at Carnegie Mellon University. Some teams around the world took the CERT term and other teams used the term Computer Security Incident Response Team (CSIRT) to point out the task of handling computer security incidents instead of other technical support work. The terms CERT, CSIRT, Incident Response Team (IRT), Computer Incident Response Team (CIRT) and Security Emergency Response Team (SERT) have been used interchangeably in the literature to refer to teams that aim to mitigate the impact of a potential major information security incident.

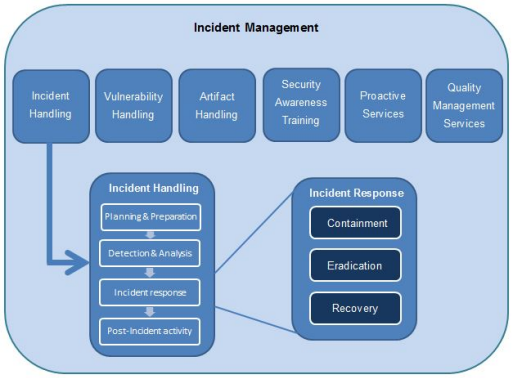

Fig. 1: Incident Management, Incident Handling and Incident Response relationship

TABLE I: Incident management models [9]

	Capabilities		
	Organization side	Provider side	Outsourced
Execution	Full-time Part-time Virtual team	Full-time Part-time Virtual team	Partially outsourced Fully outsourced

Incident management is part of a comprehensive security programme for information security governance [3] [12]. Killcrece et al. [13], emphasize that incident management is not purely an IT issue, but a wide overview of the organization's security, risk and IT management functions. Alberts et al. [14] explains that incident management encompasses incident handling, incident response and a larger set of activities such as vulnerability handling, artefact handling, security awareness training as well as other proactive services and security quality management services.

Chichonski et al. [1] and Maj et al. [3] present Incident handling as a whole lifecycle where incident response is one of the phases. Incident response is an organized approach to react to a security breach or attack. The goal is to contain, eradicate and recover from the situation in a way that limits damage and reduces recovery time and costs. Fig. 1 explains the relationship between incident management, incident handling and incident response.

A. Incident management models

Reyes [9] classified the incident management models according to an organization's capabilities, human resources and expertise (See Table I). The outsourced incident management model is usually followed by organizations focused on their core activities or by organizations looking for cost reductions. The focus of this paper is on the outsourced incident management model.

The incident management could be partially or fully outsourced in this model. Selecting a partially outsourced approach could be based on the lack of certain expertise or when is more convenient to use a third party to provide a particular service. On the other hand, fully outsourcing incident management would be an option for those organizations that want to focus uniquely and completely on their core services and rather outsource anything else.

B. Managed Security Service Provider

Outsourcing incident management services is not an option that all organizations would consider, since it may be perceived as providing control and access to the digital assets. However, outsourcing incident management services is all about a security partnership with one or more trusted third parties.

Managed Security Service Providers supply organizations with expert teams and systems, improvement in performance, reduction in capital investment technology and resources, and meticulous activities to exhibit to auditors and regulators. Depending on the contracted services, MSSPs are able to provide support to the organization or (if existent) the organization's incident management team to manage incidents and to supplement or support the existing security infrastructure.

Ferrara and Hayes [15] categorized MSSPs in three categories, based on their size and capabilities. The first category involves the largest enterprise-class providers. These MSSPs provide multiple security operation centres (SOCs) in multiple geographic locations, proprietary or significant enhanced technology, full portfolio of standard services and multi-language support. The second category has the emerging MSSPs. These MSSPs have one or two SOCs, significantly enhanced technology, full portfolio of services and language support in one to two languages. Finally, the third category includes many smaller firms that serve the small business market. These companies have a single SOC, no threat intelligence services unless reselling another company's service, narrow portfolio of services and support in a single language.

V. Results

This section presents findings from the case study. The collected data was prepared in a common format and categorized based on key themes.

The findings are organized based on three different stages: Pre-operation, Operation and Post-operation. Pre-operation refers to the stage where an organization has not created a contract with any provider to acquire incident management services. Operation describes the stage where there is an ongoing contract between the customer and the provider to outsource any kind of incident management services. Finally, the Post-operation stage deals with a normal contract completion or an early termination.

Organization A describes that good communication with internal incident management teams depends on the customer's forensic readiness, meaning that the customer is prepared and the stakeholders are involved in the case. If there is not a proper working model in the internal incident management team, there might be communication conflicts due to a lack of internal communication.

A customer that has security controls in place, trains its people, has implemented security awareness and knows what might be the threats gets more benefit of the outsourced incident management services. Organization E describes that when internal incident management teams are mature and self-sufficient, they look for assistance in services that are too complex. Organization A and C explain that outsourced incident management services could benefit an internal incident management team by providing it with more man-power, specialized services, managerial skills, a global perspective on threats and multiple sources of intelligence. However, in some cases it might affect internal teams that are trying to respond in the same manner if there are not clear lines of responsibility in terms of which team does what type of tasks. Besides some internal incident management teams might get affected by a reduction of staff.

Organization B comments that current incident management teams benefit from participating on discussions and inputs coming from the provider getting a different perspective in order to make decisions and reach agreements to deal with an incident.

Organization D highlights that some internal incident management teams might perceive the MSSPs as the help needed to prevent being fired when an incident is out of control.

Organizations A and D describe that they offer different types of SLAs in terms of different services. Organization A's responsibilities and penalties are dependent on what the customer is looking for and is willing to pay. The penalties differentiate on what services are outsourced, traditional managed security services or managed incident handling services, the level of the incident missed and the severity of the attack.

Organization B explains that the roles and responsibilities are dependent on what the client wants, the higher the SLAs the more they have to pay because it requires more staff. Organization B offers different types of SLA's not only in terms of different services but also according to the environment (production, test, development, etc.). The SLAs related with the production environment have higher cost and penalties than the rest of the environments. The penalties at the SLAs might differ from account to account. However, Organization B has compensation agreements, meaning that if an SLA is missed and there is a penalty, the compensation agreement could be used in order to condone the penalty as long as the compensation agreement is achieved.

Organization C has very specific SLAs for incident reporting or detection. If there is an incident or suspected incident, there is an escalation process to notify the customer, which is done by phone or by other means, based on its severity. But Organization C uses a different set of SLAs when it comes to incident response. Responsibilities and penalties are dependent on what is being offered and what the consequences are for the customer.

Organization E considers that there is no way to promise some customer that the provider's resources will be on site within a very specific amount of time. Everything is done of best effort and there are no artificial time limits. There is no way that a provider can promise to get to the bottom of something in an investigation in a certain period of time because each situation is different. It is hard to state SLAs because there is no level of predictability in these kinds of situations.

A. Pre-Operation

1) Identifying the services needed.: Many of the services are named differently by different providers which makes it more difficult for non-security aware costumers to find out the right services. Organization A recommends to make an in depth search of the services and then get an independent view from a third party, helping to understand what their strengths and weaknesses are and what might be suitable for the company. Organization C recommends that providers should be clear about where these services are located in the incident management process, where the starting point is, where the ending point is and what are the resources required from the customer in order to implement the services. Organization D recommends providers to devote time helping potential clients to understand how what they are doing is different from what others do and what some of the differences in their proposal are.

2) Choosing the right provider.: Companies are not aware of the broad diversity of providers that can offer to them incident management services. Organization A advises the companies to have a subscription or a working relationship with an analyst company or a neutral third party in order to get an independent view of the providers, helping to understand the MSSP market segmentation, provider's capabilities, flexibility and customer satisfaction.

3) Taking into consideration the staff morale.: The staff morale might be affected by the decision of outsourcing services that were previously run in-house. Organization B recommends involving the staff, and making them understand why the decision was made and try to make it positive.

4) Adapting to a foreign language communication when using global outsourced services.: Outsourcing services to global companies might impact the internal communication, since the staff might not be used to talking to people in another language such as English. Organization B recommends taking the internal communication into account when choosing a service provider.

5) Predicting resources and justifying them inside the business.: Customers may have a very difficult time predicting how much resources or help they are going to need and justifying it within their business. Organization E advises to take advantage of cyber-attacks reported in newspapers as headlines or in the news to make justifications easier.

B. Operation

1) Providing emergency response services to new customers.: Emergency response services are those that companies can call to during 24 hours every day of the year when they have an emergency. Organization A advises that experienced security professionals which have developed their

skills through different cases are the most suitable to provide help quickly in an unknown infrastructure, being fast and efficient on analyzing what happened, how can it be stopped and finding out what systems are in scope, in order to make the right choices for the response. Organization C describes that some customers prefer to engage multiple providers when emergency response services are required.

2) Having appropriate staff to provide response to emergency response calls.: MSSPs require having people available to respond when needed. Organization C advises that providers should be prepared to provide the appropriate people at the appropriate time, since their staff might be actively engaged in different tasks. Providers should have at least enough staff for those costumers that have contracted services.

3) Communication between external and internal incident management teams.: Internal communication within an incident where clear roles and communication mechanisms have not been established in the internal incident management team can cause communication conflicts. Organization A describes that it is important that the customers have developed some forensic readiness and incident management planning describing IRT roles and responsibilities.

4) Reaching global support when system breaches involve global companies.: Some companies might have complex systems either in their internal infrastructure or due to the fusion with other companies. When there is a breach in global companies or in companies with complex systems, such as cloud services, it might demand to get the log files involved located in different countries. Organization A recommends not looking at the whole company, but first finding the breach and then working the way through it and through the systems. If there are complex systems involved in the breach, only then global resources might be required.

5) Combine the strategic information and the intelligence.: Not all vendors have access to the same multiple sources of intelligence or the knowledge on what to do with it. Organization A describes that the quality of the input that you have access to as a vendor is a big differentiator, but then only by combining it with strategic information either from history or from experience, is when meaning can be extracted. Organization E advises that consuming intelligence will provide with detection of the right kind of anomalies and indicators of compromise to stop targeted attacks.

6) Implementing massive security services that will work without false positives.: Many customers want to get security services alerting only about the real issues and not being alerted by stuff that is not relevant. Organization A describes that it depends on the quality of the services but this would achieved once a broader integration of IT, network and security systems occurs.

7) Keeping the customers.: Customers might switch providers due to not getting the agreed service or because the service is or becomes too expensive. Organization A describes that in order to keep a customer it is important to build a trusted relationship between the provider and the customer.

8) Cultural differences might impact the working behaviour.: Offshoring is the relocation of an outsourced service from one country to another that provides cheaper labor costs. The cultural differences in those outsourcing destinations might impact the communication and the working behaviour in the provider's staff. Organization B explains that having workers with big cultural differences demand follow up activities and inter-cultural communication in order to understand the differences and get the job done.

9) Unavailable offshore personnel working in countries with natural, societal or political risk factors.: Different circumstances such as natural disasters, strikes or riots among others might restrict offshore workers to reach their working place. Organization B describes that having offshore offices spread over different locations is a good way to spread the risk and not have an impact on the offshore services provided.

10) Multiple providers interaction during an incident.: Customers may have multiple providers supporting the same incident which, even if they are assigned to do different tasks, can have some overlap. Organization C recommends that there should be some hierarchy involved when multiple providers are engaged in the same incident, to make sure that somebody is in charge and perhaps solve overlapping tasks. Organization E describes that the customer should be the one dictating how the investigation would be done and defining the separation of duties to be handled by the companies that are brought in.

11) Collecting logs from systems and infrastructure.: Customers might not be logging what is happening in their infrastructure. The use of logs is something that does not necessarily require many resources, but it provides great help when having an incident. Organization D advises to collect sufficient logs and data in order to facilitate and improve the customer's incident response process. This will allow verifying the information of an incident and would significantly speed the provider's response enabling some response functions to be performed remotely.

12) Remote response enabled by agents.: Customer's IT departments might be reluctant to the use of agents because for every incremental bit of complexity on an endpoint there is potentially a large percentage of customer service calls, help desk calls, and an increase on the time of evaluating new software or operating system releases. Organization D and E recommend working with customers to help convincing their ultimate decision maker as to why the benefit of running the agent at the endpoint is greater than the cost.

13) Lack of skilled personnel.: Shortage of people with capabilities for incident response activities. It is difficult to hire as many people as is needed. Organization D advises to hire more junior talent to develop their skills providing them with formal training and in-depth hands-on experience. Organization E advises to create bonds with universities and research groups to find dedicated people and train them.

14) Incident response roles are not clearly defined.: Incident response roles are not clearly defined in the industry, when hiring incident response experts there is a wide variation of the capabilities, level of experience and expertise that is

needed. Organization D recommends defining internally what these roles actually are for the company's needs. It is important to understand, when hiring new personnel, what they really have experience in and how that is related to what it is needed at any particular point.

C. Post-Operation

1) Understanding the customer needs and expectations when switching providers.: Not understanding the new customer's expectations and its infrastructure could make the transition challenging for the provider receiving the new costumer and deteriorate the relationship from the beginning. Organization A emphasizes the importance of getting familiar with the infrastructure both at the customer and previous provider's facilities. It is important to understand what the critical assets are, what does the customer wants to protect and where the previous provider failed. The more the provider knows about the customer then the better it would be in shape to provide protection and build a trusted relationship between the parties. Organization C describes that the provider needs to understand the new customer's challenges in order to identify the services that can be offered in that category and propose something to address them based on their prior experience.

2) Knowledge transition of customer services from one provider to another when a customer changes provider.: Providers might be reluctant to pass knowledge that took many years to get. Some of this knowledge might not be documented and does not reach the new provider. Organization B describes that providers might transition the problem knowledge that they are obliged to but not the rest. Having a proper documentation and a continuous revision of it during the meetings with the customer might help to keep everything documented so that there won't be any gaps when a provider transition will occur. Organization D highlights that the new provider should be aware that the previous provider may not have much incentive to participate on the process since they are losing a contract.

VI. Conclusion

This paper has described interviews with five large managed security service providers (MSSPs) in the global market.

Outsourcing incident management security services is a viable option to get security competence for responding to today's threats. Outsourcing incident management services seems to be a good option for small and medium size organizations that don't require tailored services. These organizations can reap affordable comprehensive security without investing in new infrastructure or being burdened by deployment and management costs. Large organizations are benefiting by specialized services or by having the chance to focus on tasks that demand specialized skills instead of repeatable tasks. Tailored solutions are not easily achieved by outsourced services. It is a complex process that requires both internal and external staff to accomplish.

All organizations can evaluate and assess what MSSPs offer according to their needs. However, the service's descriptions at the provider's websites are unclear and most of the times confusing. Mapping those services to either the incident management model, the Observe-Orient-Decide-Act (OODA) decision-making life-cycle phases, or the kill chain framework phases will enable better understanding of what the customers are lacking to increase the effectiveness of their organizational cyber-defense capabilities.

Knowledge transition of customer services from one provider to another requires proper documentation. This documentation is not effectively done, according to some of the interviewees, and in some cases there is knowledge that doesn't reach the new provider. Therefore exchange formats between providers to transfer the customer services knowledge could help to guarantee the customers that their data will be properly handled during and after the transition. A public file format for exchange of customer services knowledge should be developed to automate as much of the knowledge transition process as possible. It would make cross-organizational coordination more efficient and cost effective.

References

[1] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," *NIST Special Publication*, vol. 800, p. 61, 2012.

[2] "ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management," International Organization for Standardization (ISO), Geneva, CH, Standard, Sep. 2011.

[3] M. Maj, R. Reijers, and D. Stikvoort, "Good practice guide for incident management," 2010.

[4] "British Standards Institution. BIP 0107:2008 foundations of IT service management based on Itil V3," British Standards Institution (BSI), UK, Standard, 2007.

[5] F. Siepmann, *Managing risk and security in outsourcing IT services: Onshore, offshore and the cloud*. CRC Press, 2013.

[6] J. Sherwood, "Managing security for outsourcing contracts," *Computers & Security*, vol. 16, no. 7, pp. 603–609, 1997.

[7] I. A. Tøndel, M. B. Line, and M. G. Jaatun, "Information security incident management: Current practice as reported in the literature," *Computers & Security*, vol. 45, pp. 42–57, 2014.

[8] J. Allen, D. Gabbard, C. May, E. Hayes, and C. Sledge, "Outsourcing managed security services," DTIC Document, Tech. Rep., 2003.

[9] A. Reyes, "Incident Management in Outsourcing," NTNU, Project Report (Minor Thesis), 12 2014. [Online]. Available: http://sislab.no/projects/outIR/outIR.html

[10] "ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements Preview," International Organization for Standardization (ISO), Geneva, CH, Standard, Nov. 2013.

[11] "ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls," International Organization for Standardization (ISO), Geneva, CH, Standard, Oct. 2013.

[12] W. Brotby, J. Bayuk, and C. Coleman, "Information security governance: guidance for boards of directors and executive management," 2006.

[13] G. Killcrece, K. Kossakowski, R. Ruefle, and M. Zajicek, "Incident management," *Build Security In*, 2005.

[14] C. Alberts, A. Dorofee, G. Killcrece, R. Ruefle, and M. Zajicek, "Defining incident management processes for csirts: A work in progress," DTIC Document, Tech. Rep., 2004.

[15] E. Ferrara and N. Hayes, "The forrester wave: Emerging managed security service providers, q1, 2013," *Forrester Research, January*, 2013.