Author version, final version published in Proceedings of IEEE CloudCom 2015, Vancouver BC,
http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?reload=true&arnumber=7396204

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.

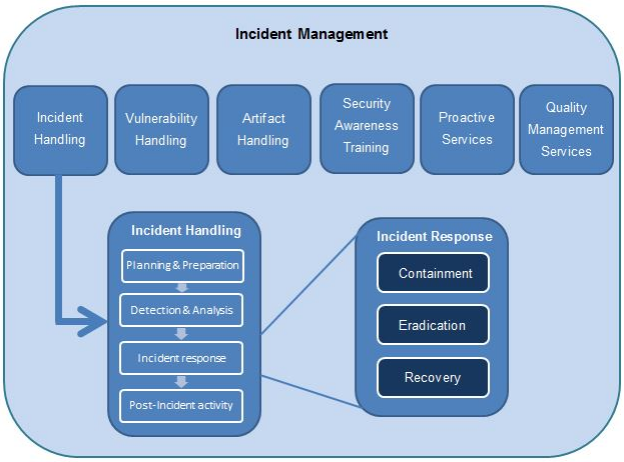

Fig. 1: Incident Management, Incident Handling and Incident Response relationship

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.