Author version; final published in Procedings of Availability, Reliability and Security (ARES), 2015 10th International Conference on, pp.467-473, 24-27 Aug. 2015, http://dx.doi.org/10.1109/ARES.2015.38

# How Much Cloud Can You Handle?

Martin Gilje Jaatun and Inger Anne Tøndel
SINTEF ICT
Trondheim, Norway
Email: {Martin.G.Jaatun,Inger.A.Tondel}@sintef.no

***Abstract*—Outsourcing computing and storage to the cloud does not eliminate the need for handling of information security incidents. However, the long provider chains and unclear responsibilities in the cloud make incident response difficult. In this paper we present results from interviews in critical infrastructure organisations that highlight incident handling needs that would apply to cloud customers, and suggest mechanisms that facilitate inter-provider collaboration in handling of incidents in the cloud, improving the accountability of the cloud service providers.**

***Keywords*—*Incident response, Cloud computing, accountability, security, privacy***

## I. Introduction

One popular visualisation of Cloud Computing is "outsourcing on steroids" [1], and although this is somewhat of an over-simplification, it is a useful starting point for discussion: What differentiates incident handling in the cloud from other outsourcing when bad things happen?

We maintain that it is not possible to create a computer system that is 100% secure. This implies that if there is someone who sees the value of breaking into your systems, they will eventually succeed – and you must therefore assume that information security incidents will take place in your system. Especially small and medium-sized businesses will usually experience a security improvement when moving corporate systems to the cloud [2], as they will get a provider with dedicated security personnel who are available 24/7, versus a part-time administrator who additionally serves as help desk, concierge, bus driver, handyman, etc.

On the other hand, the handling of incidents in the cloud is difficult because there is often a large distance (physical and logical) to the provider, and it is consequently difficult to involve the provider when something happens. This also means that you do not necessarily have access to forensics; cloud solutions are often based on multi-tenancy, which means that data from multiple clients could potentially exist on a given infrastructure, and it will not be acceptable to disclose (e.g.) a raw dump from a hard drive in this case. There are also unclear legal restrictions on data originating from one jurisdiction (e.g., Norway) but stored in another (e.g., USA). The picture is further complicated by the fact that there are potentially long provider chains, as shown in Fig. 1, where company A uses services from vendor B, which in turn uses the services of provider C. An incident at provider C may affect services provided to the end user via B and A, but may also affect other users not part of the same chain.

This paper is structured as follows. Section II provides a brief overview of current litterature on cloud incident management. Then, Section III explains the main phases of incident management, with an emphasis of what is particularly important in a cloud setting. Section IV presents results from interviews with companies, addressing how they cooperate with vendors and exchange incident information. Section V then goes back to the example presented in Fig. 1 and explains how an incident management tool can be used to ease incident notification and response in a cloud service provider chain. Section VI concludes the paper.

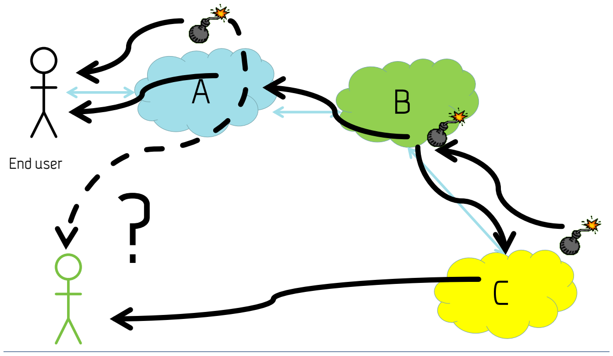

Fig. 1: Incidents in the Cloud

## II. Background

There is surprisingly little literature in this area. The Cloud Security Alliance Security Guidance report [3] has a chapter on incident handling that covers many aspects of the relationship between a Cloud Service Provider and a customer, but it does not take into account that the service can be delivered as part of a chain. Grobauer and Schreck [4] identified many challenges to incident response in the cloud, but provided few actual solutions. Furthermore, as far as we have been able to ascertain, there have not been any attempts to follow up this work in the five years that have passed. A recent survey of incident management literature [5] supports this, and the importance of further research in this area is reinforced by Munteanu et al. [6]. The best-known "standards" for incident management (ISO/IEC 27035 [7], NIST SP 800-61 [8], ENISA Good Practice Guide for Incident Management [9]) do not cover the cloud specifically, although there are many general principles here that also apply to the cloud.

## III. Incident Response Management

ISO/IEC 27035 divides incident managment into five phases, as illustrated in Fig. 2 [7]. In the following we will look at the stages one by one, and point out some recommendations. An overview of the phases can also be found in Table I.

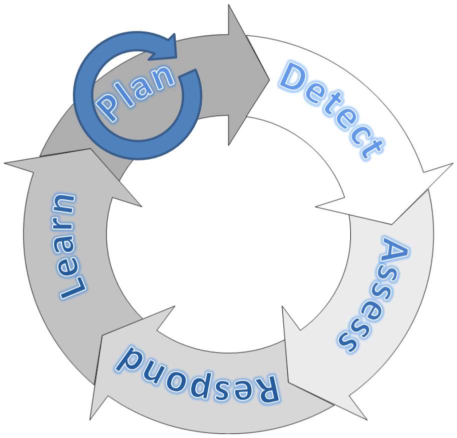

Fig. 2: The ISO/IEC 27035 Incident Response Cycle

### A. Plan

In the planning phase it is important to ascertain where the data is actually stored, and what the provider chain looks like. Secondly, it is crucial to establish an incident management plan. All stakeholders need to agree on the division of responsibility (if not, the plan need to be corrected).This also means that SLAs must include clauses for event handling, including notification requirements [10], [11].

In the cloud computing scenario, the planning phase becomes possibly even more important than in a conventional setting, since the increased complexity implies that you are less likely to get away with relying on ad hoc solutions. Trust relationships cannot be established on demand, after the fact; so in addition to ensuring that the SLA entitles you to incident information from your provider, you also need to ensure that this is true for all upstream providers. In this way, cloud providers can be accountable to their customers when incidents happen [12].

Tools that support incident handling need to be in place, and they need to be tailored to the complex information flows. In this sense, automating tasks in such a manner as to allow handlers to focus on the important stuff is vital. Furthermore, collaborative incident handling processes should be tested in drills in order to uncover practical challenges [13].

### B. Detect

Organisations should know what data sources are available to detect attacks. It may be that the provider can provide early warning, either through information on attacks on others, or with information about attacks under way against their own infrastructure. Some providers also offer Intrusion Detection Services (IDS).

### C. Assess

In the assessment phase, access to information is key. ’Snapshots’ of virtual machines can provide excellent opportunities for analysis; you can start and stop, restart, inspect memory, etc. In the planning phase, one should also have clarified what forensic support one can expect from the vendor. This includes an overview of what the provider logs, how the logs are protected against modification and fundamental things like whether clocks in the system are synchronized.

### D. Respond

Response activities may be taken by several actors in the provider chain, depending on the type of incident. As previously mentioned, the virtual machines can be frozen, stopped, restarted; this makes it ”affordable” to do things a little more brutally than you might dare to do on a conventional server. It is also possible to exploit the capabilities of the cloud directly, e.g., in case of a denial of service (DoS) attack one could theoretically spawn off new instances to handle the deluge of requests; or migrate the service to a new cloud entirely.

### E. Learn

In the learning phase, it is time to sum up; what worked well and what worked poorly? Did plans match up with reality? It is very useful to make a proper report, and share with everyone involved. The report should include a timeline of the incident, with analysis and identification of the root cause(s). Describe the short-term measures that were implemented for handling and recovery, as well as recommendations for long-term measures.

In a long and complex cloud provider chain, the sharing of such a detailed report may be politically difficult, and it may thus be necessary to filter the information in such a manner that each provider only receives information that pertains to its services.

## IV. Interview Study of Incident Management

In 2013 we performed semi-structured interviews with four critical infrastructure companies based in Norway or Sweden, with the aim of identifying their practices and challenges when it comes to handling information security incidents. All companies were dependent on ICT for collaboration and decision making across organisational and geographical borders by means of ICT. The companies represented the oil and gas sector, marine operations, energy and transportation. The interviews were based on an interview guide that covered the following topics: the background of the informant, the company’s dependence on ICT, what types of incidents the company experiences and how they are handled, what types of incidents they fear the most, how incidents are detected, need for collaboration during incident management, plans, drills, metrics and support tools. All interviews were performed on phone by one researcher, with another researcher taking notes, and the interviews were recorded and transcribed. Analysis of the interviews were done by the researcher performing the interviews. In this paper we report on results from these interviews that can shed light on the following research questions:

- What strategies do the companies use in their cooperation with vendors and service providers, both to

TABLE I: Overview of incident management phases

| Phase | Important aspects in a cloud setting | Findings from interviews |
|---|---|---|
| Plan | Understanding the provider chain. Establishing contracts and plans, and work on trust relationships. Acquiring necessary tools. | Contracts are essential, but it is challenging to establish contracts that meet the needs. Personal relations are very imiportant should an incident occur. |
| Detect | Detection capability of provider. Notification requrements on vendors, and internal ability to handle notifications. | |
| Assess | Access to information. Support from vendor. | Depend on the vendors competence: will they understand the difference between security incidents and other incidents? It is not always clear where the problem lies and what vendor should be responsible for handling the incident. Vendors may be reluctant to contribute to assessment activities if it is not clear that management of the incident is their responsibility. |
| Respond | Can exploit cloud capabilities in response activities. | Vendor cooperation may be challenging, if this is not part of contracts and the vendors are used to working together. |
| Learn | Create report, and share lessons learnt. | Contracts may need to be improved. There may be a tendency for different actors to blame each others. |

prepare for incident management and to respond when an incident occurs?

- Which actors do the companies share information with today, when it comes to incidents and the management of these, and what are their opinions on prerequisites for incident information sharing?

None of the companies used cloud services at that time. One of the interviewees represented a company that had outsourced their IT to three different vendors. Another of the interviewees represented the service provider of one of the companies. All interviewees were dependent on vendors for central business functions. Table II provides an overview of the interview subjects and the companies studied.

In the two following subsections we present input from the interviewees that were relevant for the research questions, before we discuss the relevance of the results for a cloud setting in the final subsection. An overview of results relevant for the five incident management phases of ISO/IEC 27035 can be found in Table I.

### A. Interaction with Vendors and Service Providers

Based on the interviews, we identified the following main strategies to deal with vendors:

- Contracts
- Routines
- Involving top management
- Building relations and trust

In many cases the interviewees explained how they, during incident management, had experienced that their current contracts with vendors did not meet their needs. As examples, the service provider of company C-D explains that their contract with C-D includes response guarantees, but that their vendors does not live up to that response time. Some of the vendor decisions and contracts have been made at a time when the C-D requirements were different. Updating these contracts is thus a priority. Also C-A told about an incident in which they were not satisfied with the response time of the anti-virus company. The interviewee from C-A said the anti-virus vendor did not deliver according to contract but that they also could have had a better contract with the vendor.

Two of the respondents explained that it could often be challenging to know which vendors should be involved when an incident occur. Company C-C performs multisourcing, and as a consequence three to four different vendors can be involved in incident management depending on the system that is hit. One of the vendors is responsible for the helpdesk, and incident management is organised by that vendor. Then that vendor need to inform the other relevant vendors that they have to respond to an incident. The interviewee explains that they have felt their way, they know what is not working. The interviewee stated: *“It is very, very important to have contracts regulate how error management and incident management should be performed, no matter the type of incident, and that if you have more than one vendor they must be forced through contracts to cooperate. If not, it will never work!”*

Routines related to incident response in many cases include how to interact with vendors. The service provider of C-D tells about this, both when it comes to following up on SLA requirements, and for communicating when an incident occurs. They have regular meetings with their customers, and have defined lines of communication that includes the management level. Company C-C explain that, in case of an incident, they establish a task-force and have routines for which people to involve and which meetings to arrange, with phone meetings every hour, and more if needed. Especially the service provider of C-D talks about how they escalate to the management level in case their vendors do not provide the necessary support when an incident occurs, and that collaboration with vendors in general often includes the management level.

It seems that the vendor experiences and expectations vary between the companies studied. Company C-B seems rather positive when it comes to how vendors improve the company’s preparedness for information security incidents. As an example, the interviewee from this company was quite concerned regarding their internal capacity to deal with incidents, especially outside of office hours, but were confident that vendors would be able to help at any time, as their contract with vendors was in force 365 days a year. Others are more concerned, e.g about the competence of their vendors. Company C-B explain that when they experienced a DDoS incident, they

TABLE II: Overview of companies

| Company | Interviewee | Description |
|---|---|---|
| C-A | Information security manager | Multinational. Depend on vendors. Strong information security competence inhouse. |
| C-B | Information security manager | Regional. Depends on vendors. Limited inhouse information security competence |
| C-C | Security manager | National. Outsourcing to several vendors. |
| C-D | Application department manager at the service provider of the company | Multinational. Outsourcing to service provider that only serves companies in the same corporation. That service provider in turn relies on a number of vendors to provide the necessary services. |

found that it took a long time for their vendors to find out what caused the problems. They state that their vendors has problems understanding that it may be an IT security problem if something happens in the system, and not just a service that is unavailable. They are working with their vendors to improve awareness on security. Also the interviewee from this company (C-B) sees collaboration issues with vendors as inevitable to some extent, stating: *"I guess there is no company in the world that has outsourced their IT, that thinks collaboration with their service provider works well. I have never heard about that. So there is always challenges. The vendors want to do as little as possible. The more they do, the more it costs for them, so they want to do as little as possible. And we, that buy services from them, want them to do as much as possible, and we would rather not pay them. There is always a challenge to come to agreements so that we get what we pay for."*

No matter what their expectations are, building and maintaining a close relationship with their vendors seem to be important. For company C-B that is concerned about the availability of internal resources, it is important that the key personnel at their vendors, those that know C-B's business and systems, are available should something occur. For company C-C, that performs multisourcing and relies on vendor collaboration, it is important to build trust also between the different vendors. When asked if the vendors blame each others, and don't want to start handling the incidents, the interviewee from C-C stated: *"Yes, of course! When problems are difficult to solve, and it is not given that there is an error in the server or in the software, then it can take time for them to be able to cooperate sufficiently to find out what the problem is. This goes better and better, but in the beginning this was a big problem because then they really blamed each other. And it could take time. But as I perceive it, this has become considerably better, but it is a slow process that you need to work on all the time, and that is what the incident manager is doing all the time – finding out how to do this better."*

### *B. Incident Information Sharing*

In addition to communication with vendors and internal communication about the incident, the companies told about incidents when they shared information with national Computer Emergency Response Teams (CERTs) or other companies. As examples, companies may have equipment at installations where another company is responsible for IT. Company C-A told about a watering hole incident where they contacted other companies they knew of that could also be hit. Tips about incidents may likewise come from CERTs or other external actors. For some incidents, there may be a need for external specialist competence, e.g., on reverse engineering or forensics. Company C-A also explains that they sometimes take part in national emergency drills that include information security.

Company C-A in particular were clear about the importance of sharing incident information. In the watering hole incident, they benefited due to their willingness to share information, stating: *"What worked really well this time was in fact the collaboration with our partners. Both Microsoft who was very professional and very good to deal with when it comes to things like this, but also the other actors that we share information with. Because what became clear quite soon was that there were more actors than us that were hit by the same thing. And we solved the puzzle together – that is, we added some pieces, and others added other pieces, and that way we were able to complete it much faster than we would otherwise."* At the same time they are clear that information sharing is not always working, and is not prioritised by all actors. For the same incident, the interviewee from C-A also stated that something that did not work well was information sharing with some of the anti-virus vendors they used, as they were slow on sharing information and very slow in issuing a fix. Again, it comes back to relations and trust as essential for successful incident information sharing: *"Externally it is a bit like . . . depends on who you involve . . . for example [the national CERT] NorCERT that we work a lot with, that usually always works well. I do not think we have examples that it worked bad with them. When it comes to other companies or others that we share information with or rely on, then it varies, it depends on who it is, because then it depends on the relations. With some we have come far, while others keep their cards close to their chest."* The interviewee from C-A explain that information sharing (e.g. in the form of sending samples to Microsoft and anti-virus vendors) has become more common and that there is more openness about incidents than before. He states that in their company they have decided that they want to share, because they believe it will benefit everybody, including themselves. So they try to find others that also want to share, so that they can warn each other.

Internally in the companies, there is often tool support available for documenting and reporting incidents. However, the interviewee from company C-A explains that they are reluctant to using these tools because of confidentiality issues. To illustrate, the Computer Security Incident Response Team (CSIRT) does not have overview of who has access to the information they register in such a system (e.g., admin users). As a result they anonymise the information they put in this system as much as they can, and instead use an internal encrypted site for more detailed documentation.

### C. Relevance for Cloud Scenarios

As none of the companies we surveyed used cloud services at that time, it is important to assess to what extent their experiences are relevant for cloud scenarios. We assume that a migration towards increased use of cloud services will result in an increased need to exchange incident information, in form of notifications as well as cooperation during incident management. Work on establishing trust, as well as on having contracts, routines and systems that support information exchange will thus be even more important.

Although the companies in the survey seems to have rather close distance to their vendors (compared to what you would expect in a cloud setting) they still experience problems, especially regarding contracts but also when it comes to relations and trust. Top management involvement can then be used as a strategy, when vendors does not meet the company's expectations regarding incident management. This strategy seem to work well for some of the surveyed companies, but will likely be more difficult to apply in a cloud setting where the distance to the provider is longer. Improved contracts, where incident management responsibilities are made more clear, can be important to reduce the need for top management involvement. But these contracts also need to be followed up, so that the companies can trust that they receive what they pay for.

The companies that rely most heavily on outsourcing seem to spend a lot of time on following up on vendors. As the number of vendors as well as the importance of the vendor relationships increases, it will likely be necessary with more efficient ways on following up on vendors, or in case of providers, to follow up on customers. This can come in form of routines and the way the follow-up of these business relationships is organised, but automation and tool support can also play an important role, especially when it comes to common and low-impact incidents and the exchange of data related to SLA metrics.

As people working on information security incident management are likely to be highly aware of security risks, it is essential for willingness to share incident information that there is an ability to share information in a secure manner. The security of the information exchange should be transparent, so that the security experts of the company can understand the security level and trust the implementation of the exchange system. This will especially be important for any tool offering incident information exchange between actors in the provider chain. However, trust issues are still important between the companies involved as well as the people working in the companies. Maintaining such relationships will likely be more difficult in a cloud setting. Mandatory data breach notification laws can overcome some of the reluctance towards sharing. But still, if there is no trust relationship the information shared will likely be only the minimum required, and not necessarily the information necessary for effective cooperation during incident management.

## V. The role of tool support: Back to the Example

From the interviews, and the discussion of their relevance for cloud scenarios, we identified the following areas that will be important for successful incident management:

- Improved contracts, as well as ways to follow up on contracts
- More efficient ways to organise vendor interaction, including incident information exchange
- Secure means of exchanging incident information
- Trust relationships between organisations as well as the individuals working there, to ensure willingness to share the necessary information

Having a tool for incident information sharing can be beneficial as it supports secure exchange of such information and eases automation of responses to simple and common incidents. As an example, experiences from LRZ-CSIRT [14] show potential benefits of automatic processing of incident alerts, something that was made possible due to standardised XML-based notifications from DFN-CERT. The use of a tool can also ease access to relevant information, a problem that is not limited to cloud scenarios. As an example, in a study by Ahmad et al. [15], an information security manager stated that the sharing, or rather the finding, of information was one of the most challenging parts of her job. However, it is unlikely that a tool can solve all problems with incident communication. In an electronic survey among system administrators in large scale IT service organisations, de Souza et al. [16], found that people were the most important sources of information in working with complex incidents. In only 33 % of the cases was the information from the incident tool sufficient. In addition, automating incident information sharing may not be desirable in all cases, as the company may want to have more control over what information is sent to customers and other business connections.

We envision that businesses in the cloud provider chain could benefit from tool support for the following purposes:

- *SLA follow up:* To have an overview of SLA requirements related to incident management, both the requirements that the organisations has promised to fulfil for their customers and the requirements that the organisation has posed upon its providers. And, additionally, to follow up on these requirements (through metrics), to be able to detect whether or not the SLA requirements are met.
- *Incident notifications:* To be able to receive and send incident notifications in a standardised format, and in an automatic fashion, based on notification requirements in SLAs, as well as regulatory requirements.
- *Incident collaboration tools:* To facilitate cooperation and two-way incident information exchange between actors in the provider chain, when cooperation and discussions are needed for specific incidents.

The need for this tool support comes in addition to any incident management tool necessary for efficient and effective incident management in a general case (such as detection tools, ticketing systems, decision support systems, etc.). Support for incident notification is an important starting point, and in the following we provide more detail about how such functionality may be realised.

One of the many things that the literature [4] identifies as a deficiency is information sharing along the entire provider chain. In the example we started with, we have the situation illustrated in Fig. 1, where a user has to deal with the provider chain A-B-C. We therefore need a mechanism where provider C can inform B about events that affect services B buys from C. B must then aggregate this information (and other information), and make it available to A, who must do the same to the end user. It is likely that the interface with the end user must be quite different from the provider interfaces, as indicated in Fig. 3, and may need to involve manual processing.

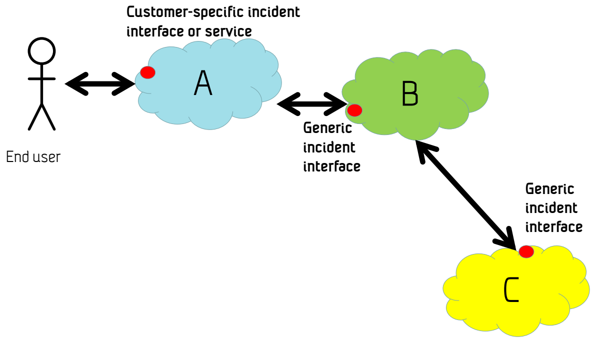

Fig. 3: Incident Interfaces

Kampanakis [17] provides an overview of formats that can be used for exchange of incident information. In our work so far we have mainly considered the following protocols as candidates for communication between providers:

- **Intrusion Detection Message Exchange Format** (IDMEF) [18] is designed to transfer incident information from Intrusion Detection Systems (IDS). As such it may be too constrained for our purpose, since it assumes all incidents are a result of an external attacker. In our case we must also consider incidents that originate from providers who break (consciously or otherwise) policies or SLAs negotiated with customers.
- **Incident Object Description Exchange Format** (IODEF) [19] has been designed to facilitate information sharing between CSIRTs, but is just like IDMEF focused on external attackers. It may not be granular enough for our purpose, but could possibly be extended to suit our needs.
- **CSA Cloud Trust Protocol** (CTP) [20] is primarily designed as a tool for cloud customers, and in addition to a request/response protocol, it also makes it possible for customers to subscribe to certain events. CTP is still under development, but it currently looks like parts of it could be used to support our incident sharing scheme.

In addition we have considered the use of **Transparency Log** (TL) [21]. TL is (as the name suggests) primarily a logging mechanism, but may also be used as a secure channel between two parties. However, for our purpose it may be less suited, since there is no automatic notification to the recipient; instead, it must keep polling to determine whether new information has been added to the log store. None of the available protocols are a perfect match for our scheme, but IODEF and CTP (or a combination of the two) are candidates for further study.

Each provider in the chain need to have an Incident Response Tool (IRT) that is able to receive and send incident notifications in the agreed upon format. The IRT must be able to access the generic incident response interface as illustrated in Fig. 3, configuring alerts for incidents that affect their customers. E.g., CSP A must be able to subscribe to alerts from CSP B that relate to services that CSP A resells to their customers (broadly speaking). The IRT must in turn pass on incident information to its downstream customers via the incident interface. Apart from this, the IRTs of different providers do not need to be the same, but can be tailored to the individual needs of the different providers.

For the success of an automated incident notification tool, it is essential to have a good understanding of what information is necessary to assess and respond to incidents in a cloud environment. There exists some research on this in the general case, e.g., on what information it is important to establish a shared mental model of between incident responders [22]. We are however not aware of research on this that take the cloud environment into account.

## VI. Conclusion

In this paper we have presented interviews that emphasise the need for sharing incident information along the cloud provider chain. We have suggested an incident response tool that will build on standard protocols to improve the quality of the incident information that flows back to the user, thus improving the accountability of the cloud service providers.

In future work we will extend our model to also cover notification of end users via a cloud provider administration panel.

## Acknowledgements

We are grateful for the support of the A4Cloud project partners. Also thanks to Åsmund Nyre for contributions to evaluating the potential protocols. This work has been funded by the European Commission (grant nr. 317550) and the Research Council of Norway (grant nr. 201557/S10).

## References

[1] M. G. Jaatun, Å. A. Nyre, S. Alapnes, and G. Zhao, "A Farewell to Trust: An Approach to Confidentiality Control in the Cloud," in *Proceedings of the 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless Vitae Chennai 2011)*, 2011.

[2] M. G. Jaatun, P. H. Meland, K. Bernsmed, H. Castejón, and A. Undheim, "Cloud Security Whitepaper – A Briefing on Cloud Security Challenges and Opportunities ," October 2013. [Online]. Available: http://www.telenor.com/media/articles/2013/safe-in-the-cloud/

[3] "Security Guidance for Critical Areas of Focus in Cloud Computing," 2011. [Online]. Available: https://cloudsecurityalliance.org/guidance/

[4] B. Grobauer and T. Schreck, "Towards incident handling in the cloud: Challenges and approaches," in *Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop*, ser. CCSW '10. New York, NY, USA: ACM, 2010, pp. 77–86. [Online]. Available: http://doi.acm.org/10.1145/1866835.1866850

[5] N. H. A. Rahman and K.-K. R. Choo, “A survey of information security incident handling in the cloud,” *Computers & Security*, vol. 49, no. 0, pp. 45 – 69, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404814001680

[6] V. Munteanu, A. Edmonds, T. Bohnert, and T.-F. Fortis, “Cloud incident management, challenges, research directions, and architectural approach,” in *Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on*, Dec 2014, pp. 786–791.

[7] “ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management,” 2011.

[8] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer Security Incident Handling Guide,” National Institute of Standards and Technology Special Publication 800-61, 2012.

[9] ENISA, “Good practice guide for incident management,” 2010. [Online]. Available: http://www.enisa.europa.eu/act/cert/support/incident-management

[10] M. G. Jaatun, K. Bernsmed, and A. Undheim, “Security SLAs  an idea whose time has come?” in *”Proceedings of the International Cross Domain Conference and Workshop (CD-ARES)”*, 2012.

[11] P. H. Meland, K. Bernsmed, M. G. Jaatun, H. N. Castejón, and A. Undheim, “Expressing cloud security requirements for slas in deontic contract languages for cloud brokers,” *Int. J. of Cloud Computing*, vol. 3, no. 1, pp. 69 – 93, 2014.

[12] M. G. Jaatun, S. Pearson, F. Gittler, and R. Leenes, “Towards strong accountability for cloud service providers,” in *Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on*, Dec 2014, pp. 1001–1006.

[13] M. B. Line and N. B. Moe, “Understanding collaborative challenges in it security preparedness exercises,” in *Proceedings of IFIP SEC*, 2015.

[14] S. Metzger, W. Hommel, and H. Reiser, “Integrated Security Incident Management – Concepts and Real-World Experiences,” in *Sixth International Conference on IT Security Incident Management and IT Forensics (IMF)*, 2011, pp. 107–121.

[15] A. Ahmad, J. Hadgkiss, and A. B. Ruighaver, “Incident Response Teams - Challenges in Supporting the Organisational Security Function,” *Computers & Security*, vol. 31, no. 5, pp. 643–652, 2012.

[16] C. R. B. de Souza, C. S. Pinhanez, and V. F. Cavalcante, “Information needs of system administrators in information technology service factories,” in *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology*, ser. CHIMIT ’11. New York, NY, USA: ACM, 2011, pp. 3:1–3:10. [Online]. Available: http://doi.acm.org/10.1145/2076444.2076447

[17] P. Kampanakis, “Security automation and threat information-sharing options,” *Security Privacy, IEEE*, vol. 12, no. 5, pp. 42–51, Sept 2014.

[18] H. Debar, D. A. Curry, and B. S. Feinstein, “The Intrusion Detection Message Exchange Format (IDMEF),” IETF Network Working Group RFC 4765 , March 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4765.txt

[19] R. Danyliw, J. Meijer, and Y. Demchenko, “ The Incident Object Description Exchange Format,” IETF Network Working Group RFC 5070 , December 2007. [Online]. Available: http://www.ietf.org/rfc/rfc5070.txt

[20] Cloud Security Alliance, “ Cloud Trust Protocol.” [Online]. Available: https://cloudsecurityalliance.org/research/ctp/

[21] T. Pulls, R. Peeters, and K. Wouters, “Distributed privacy-preserving transparency logging,” in *Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society*, ser. WPES ’13. New York, NY, USA: ACM, 2013, pp. 83–94. [Online]. Available: http://doi.acm.org/10.1145/2517840.2517847

[22] R. Floodeen, J. Haller, and B. Tjaden, “Identifying a shared mental model among incident responders,” in *IT Security Incident Management and IT Forensics (IMF), 2013 Seventh International Conference on*, March 2013, pp. 15–25.