

Could the Outsourcing of Incident Response Management Provide a Blueprint for Managing Other Cloud Security Requirements?

Bob Duncan¹(✉), Mark Whittington², Martin Gilje Jaatun³,
and Alfredo Ramiro Reyes Zúñiga⁴

¹ Computing Science, University of Aberdeen, Aberdeen, UK
bobbduncan@abdn.ac.uk

² Business School, University of Aberdeen, Aberdeen, UK

³ Department of Software Engineering, Safety and Security SINTEF ICT,
Trondheim, Norway

⁴ Department of Telematics, NTNU, Trondheim, Norway

Abstract. In this chapter, we consider whether the outsourcing of incident management is a viable technological approach that may be transferable to other cloud security management requirements. We review a viable approach to outsourcing incident response management and consider whether this can be applied to other cloud security approaches, starting with the concept of using proper measurement for a cloud security assurance model. We demonstrate how this approach can be applied, not only to the approach under review, but how it may be applied to address other cloud security requirements.

Keywords: Cloud · Requirements · Measurement · Assurance · Outsourcing · Incident response · Security

1 Introduction

The cloud has been referred to as “outsourcing on steroids” (Jaatun et al. 2011), and in the following we review a proposed approach to outsourcing incident response management (Reyes and Jaatun 2015), and consider whether this approach might be transferable to other cloud security requirements, starting in this case with a particular approach to cloud security addressing the importance of proper measurement for a cloud security assurance model (Duncan and Whittington 2015e). Reyes and Jaatun (2015) indicate that outsourcing of incident management is a viable security approach for many organizations, but that transitioning between providers frequently is a challenge. Duncan and Whittington (2015e) suggest that defining proper measures for evaluating the effectiveness of an assurance model, which they have developed to ensure cloud security, is vital to ensure the successful implementation and continued running of the model. The authors recognise that responsibility must lie with the board. However, in this work, we consider the viability of outsourcing these requirements to deliver an independent assurance of delivered security.

The fundamental concepts of information security are confidentiality, integrity, and availability (CIA). Beaument and Pym (2010) provide an account of the misunderstandings prevalent in information security which arise through confusion between (declarative) objectives of (Parker and Crime 1998; Neumann 1995) information security operations with the (operational) mechanisms deployed in order to achieve these objectives. Achieving information security in the cloud is not a trivial process. There are a great many challenges to overcome and, with Pym, Duncan and Whittington addressed some of those in earlier work (Duncan et al. 2013), developing a conceptual model for cloud security assurance, where they addressed three key challenges, namely standards, proposed management method and complexity. Duncan and Whittington (2015e) extended these key challenges to address a total of six possible challenges, which we expand on in Sect. 3.

The rest of this chapter is organised as follows: Sect. 2 summarises the main points related to outsourcing of incident response. In Sect. 3, we outline the work of Duncan and Whittington which highlights the requirements to be addressed. In Sect. 4, we consider whether these requirements might reasonably be provided through outsourcing, and how we might approach this. In Sect. 5, we discuss the implications of our findings and in Sect. 6 we offer our conclusions.

2 Outsourcing of Incident Management

An organization may have several motivations for outsourcing incident management. Reyes and Jaatun (2015) list the following:

- 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 24 × 7

Reyes interviewed representatives from organizations who are transnational organizations selected based on the managed security service provider’s (MSSP) market presence (Reyes 2015; Reyes and Jaatun 2015). Six large MSSPs and an emerging one (dubbed “A” to “G”) contributed to the interviews; for more details on each MSSP, see Reyes (2015).

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 incident management services. Finally, the *Post-operation* stage deals with a normal contract completion or an early termination.

2.1 Pre-operation

Identifying the Services Needed. Many similar services have different names at different providers, which makes it difficult for customers to choose the right service. Organization A recommends making an in-depth search of the services and then get an independent view from a third party, 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 resources are 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 they are trying to address.

Choosing the Right Provider. Companies are not aware of the broad diversity of providers that offer 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 out about the provider's pro-activity, the skills and knowledge from their personnel and the methodology which their processes are aligned to.

Taking Staff Morale into Consideration. Staff morale might be affected by outsourcing services that were previously run in-house. Organization B recommends involving the staff, and making them understand why the decision was made. Organization F advises MSSPs to persuade their customers that what they are doing is to take away the repeatable processes, so that the customer's 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 Foreign Language Communication When Using Global Outsourced Services. Outsourcing services to global companies might impact internal communication, since staff might not be used to talking to people in another language. Organization B recommends taking internal communication into account when choosing a service provider.

Predicting Resources and Justifying Them Inside the Business. Customers may have difficulties 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 the news to make justifications easier.

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.

2.2 Operation

Communication Between External and Internal Incident Management Teams. If clear roles and communication mechanisms have not been established in the internal incident management team, this can cause communication conflicts. Organization A describes that it is important that the customers have developed some forensic readiness and incident management documentation 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.

Collecting Logs from Systems and 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.

Providing Emergency Response Services to New Customers. Emergency response services are available 24 h a day, every day. 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. 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.

Reaching Global Support When System Breaches Involve Global Companies. Some companies might have complex systems either in their internal infrastructure or due to mergers with other companies. When there is a breach in companies with complex systems such as cloud services, international forensics might be an issue. Organization A recommends not looking at the whole company, but first finding the breach and then working your way through it and related systems. If there are complex systems involved in the breach, only then global resources might be required.

Combine the Strategic Information and Intelligence. Not all vendors have access to the same level of intelligence. Organization A describes that the quality of the input that you have access to as a vendor is a big differentiator, but its meaning can only be extracted by combining it with strategic information either from history or from experience. Organization E advises that intelligence can help with detection 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 be 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 Behavior. 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 behavior 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.

Unavailable 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.

Remote Response Enabled by Agents. IT departments might be reluctant to the use of agents because increased complexity on an endpoint may cause increased customer service calls, help desk calls, and time for evaluating new software 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.

2.3 Post-operation

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. 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 in the process. Some cases it is needed to educate and train the new people that have been hired to perform the same services.

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 customer 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 want to protect, and where did the previous provider fail. 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.

3 The Importance of Proper Measurement for a Cloud Security Assurance Model

In this section, we summarize the Duncan and Whittington (2015e) paper on the importance of proper measurement for a cloud security model.

3.1 The Challenges

The fundamental concepts of information security are confidentiality, integrity, and availability (CIA), a concept developed when it was common practice for corporate management to run a company under agency theory. We have all seen how agency theory has failed to curb the excesses of corporate greed. The same is true for cloud security, which would suggest a different approach is needed. We have identified six key points to address: definition of security goals, compliance with cloud security standards, audit issues, the impact of management approaches on security, and how complexity and the lack of responsibility and accountability affects cloud security.

In looking at the definition of security goals, we have recognised that the business environment is constantly changing, as are corporate governance rules and this would clearly imply changing measures would be required. More emphasis is now being placed on responsibility and accountability (Huse 2005), social conscience (Gill 2008), sustainability (Ioannidis et al. 2013; Kolk 2008), resilience (Chapin et al. 2009; Chang et al. 2016) and ethics (Arjoon 2012).

Responsibility and accountability are, in effect, mechanisms we can use to help achieve all the other security goals. Since social conscience and ethics are very closely related, we can expand the traditional CIA triad to include sustainability, resilience and ethics. This expansion of security requirements can help address some of the shortcomings of agency theory, but also provides a perfect fit to stewardship theory. Stewardship carries a broader acceptance of responsibility than the self-interest embedded in agency. This breadth extends to acting in the interests of company owners and potentially society and the environment as a whole.

On the matter of achieving compliance with standards in practice, we have identified the use of assurance to achieve security through compliance and audit. With compliance, there are a number of challenges to address. Since the evolution of cloud computing, a number of cloud security standards have evolved, but there is still no standard which offers complete security, which is a limitation. Even compliance with all standards will not guarantee complete security, which, presents another disadvantage (Duncan and Whittington 2014).

The pace of evolution of new technology far outstrips the capability of international standards organizations to keep up with the changes (Willingmyre 1997), adding to the problem and meaning it may not be resolved any time soon. We have argued that companies need to take account of these gaps in the standards when addressing issues of compliance. In (Duncan and Whittington 2014), we have addressed the question of whether compliance with standards, assurance and audit can provide security, and in (Duncan and Whittington 2015d), we have addressed one of the fundamental weaknesses of the standards compliance process.

Auditing in the accountancy world has enjoyed the benefit of over a century of practice and experience, yet there remain differences of opinion and a number of problems are yet to be resolved. Duncan and Whittington (2014) provide some background on this issue. Cloud audit can not be considered a mature field, and there will be some way to go before it can catch up with work done in the accounting profession. Clearly further research will be needed in this area.

Looking at management approach, we would argue that a shift from agency behaviour to a stewardship approach (Duncan and Whittington 2015a) can go a long way to reducing the major weaknesses inherent in an agency approach to security in cloud ecosystems. We have observed that cloud service providers (CSPs) have developed their cloud business models using agency theory. Pallas (2014) suggest that agency theory models the current relationship between CSPs and cloud users very well, further suggesting this expresses all the weaknesses of agency and highlights many of the issues still faced today.

Given the potential multiplicity of actors, and the complexities of their relationships with each other in cloud ecosystems, it is clear that simple traditional agency relationships (where each actor looks to their own short term ends) will no longer be able to handle fully the security implications for users of these ecosystems. There is a clear need for developing a stronger mechanism to ensure that users of such ecosystems can be assured of the security of their information. We have addressed (Duncan and Whittington 2015a) the cloud security issue with management method, and argued that the historic reliance on agency theory to run companies can present a barrier to effective security.

In considering complexity, we have observed that since cloud computing was developed, the majority of security based research has concentrated on providing technical solutions to solve the security problem. While many excellent solutions have been proposed, cloud security can never be achieved by technical means alone.

First, the core business architecture comprises a combination of people, process and technology (PWC 2012), thus a solution which addresses only one of these key elements will always be doomed to failure. Second, a cloud user can take as many steps to secure their business as they wish, but a key ingredient in the equation is the fact that all cloud processes run on someone else's hardware, and often software too — the CSP's. The cloud relationship needs to include the CSP as a key partner in the pursuit of achieving security. Unless and until CSPs are willing to share this goal, technical solutions will be doomed to failure. Third, the additional complexities which cloud brings into the security equation must be recognised, and dealt with appropriately. Increased complexity brings with it increased risk. If this risk is not recognised, and dealt with appropriately, this will inhibit the possibility of achieving good security.

Currently, cloud users effectively have to treat cloud services as a black box, since they have no control over what goes on inside, or behind the scenes. This puts cloud users at a singular disadvantage when it comes to issues of privacy and security. Regulators are taking a far more aggressive approach to breaches, and the cloud user is the one who ends up carrying the can and getting the punitive fines issued by the regulator.

This leads to the issue of lack of responsibility and accountability. Standard service level agreement (SLA) offerings from the major players currently ignore accountability, assurance, audit, confidentiality, compliance, integrity, privacy, responsibility and security, merely offering availability as the focus of their measure of performance. The onus for measuring and proving unacceptable performance is neatly passed to the customer, which, with the inclusion of some suitably deeply buried clauses in the small print, assures the buck invariably never stops with the CSP.

Companies who are cloud users are quite properly legally held responsible and accountable to a variety of regulators throughout industry under privacy and security regulations. Fines for non-compliance are reaching punitive levels, and many regulators have extreme levels of sanction at their disposal. Yet, CSPs are not held to account for their often not inconsiderable role in such failures! This issue with CSP SLAs is not a trivial issue to address. CSPs need to provide users with assurance, through compliance and audit, that they can provide a level of service capable of meeting user requirements in confidentiality, integrity, privacy and security. CSPs should be prepared to offer cloud users performance guarantees in all their required areas, not just on availability. CSPs need to become accountable to users for meeting these requirements, by which means they will be able to demonstrate a responsible and ethical approach to their customers, and at the same time, providing an extremely robust and dependable service to all cloud users.

We further argue that the CSPs should provide monitoring tools to collect sufficient information to demonstrate that they have achieved the required level of performance, rather than leaving it for customers to find out when something goes wrong. CSPs are much better placed to do this, since cloud customers will not necessarily have access to all the systems necessary for this to happen. We

have further argued (Duncan and Whittington 2015b) that this will require a significant change in attitude from the CSPs, leading to the development of better security oriented SLAs, which will improve the approach to security for all actors within the cloud ecosystem.

This was the basis on which, with Pym, we developed a conceptual framework for cloud security assurance (Duncan et al. 2013), expanding on earlier works (Beautement and Pym 2010; Baldwin et al. 2011), which seeks to address the issues faced in trying to achieve security in the cloud, and provides a more effective means for business to achieve both cloud security assurance along with appropriate standards compliance, by providing continuous assurance through both compliance and audit. We draw on natural resource management research (Chapin et al. 2009; Kao 2007) which provides some very clear illustrations of the effectiveness of stewardship, presenting a clear systems view of the issues addressed. The framework we have proposed addresses these key challenges facing cloud users.

3.2 How Our Framework Operates

The framework functions by taking a 3 dimensional security approach to how the company is organised. On one dimension there is the business architecture, which covers people, process and technology; the second dimension covers the security properties, which extends the traditional CIA approach by adding sustainability, resilience and ethics; and the third dimension is the systems architecture of the business, which addresses the systems, services and applications used by the business, to which we must add the cloud models of infrastructure, platform and software as a service (IaaS), (PaaS) and (SaaS). The framework then identifies and addresses every point in the matrix where each of the three dimensions intersect (Fig. 1).

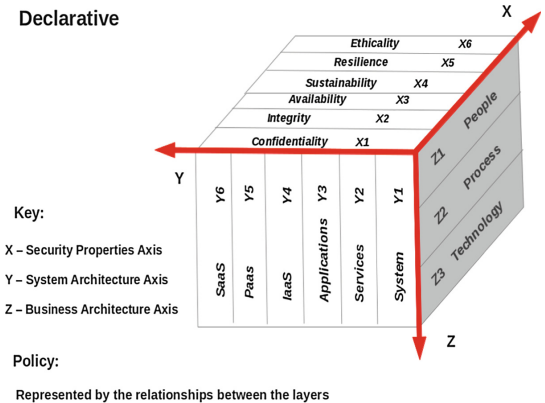


Fig. 1. A declarative cloud three-dimensional security matrix

There are 4 stages of process involved in running the model. There is the declarative stage, where management set the goals to be achieved. Next the operational stage collects data to measure how well the company is meeting these declarative goals. Then, internal audit will provide assurance through audit and compliance checks to confirm the integrity of the process. Finally, external audit will essentially double check that everything undertaken will have been compliant and thus compliance with standards can be achieved, together with the assurance that the declarative goals of management are being met.

Thus, management need to determine their declarative position on each of these intersecting points, and further, must determine how performance will be measured. Management are responsible for defining proper measurements and metrics to be used in the framework, and this is what we will now address.

3.3 How to Develop Useful Measurements

Duncan and Whittington (2015e) provide an extensive list of literature on the subject of measurement, which we will not reiterate here. We will simply focus on the development of useful measures for a company. Defining a generic set of measures is unlikely to be useful, since every business is different. This is a task for management. However, we think it will be useful to provide some general assistance by way of a few examples of how to go about it. We will start by looking at each dimension in turn.

Measuring people can be relatively straightforward. Each employee has a unique employee number, a unique computer access code and password, and access rights to whatever areas are appropriate for carrying out their job. Some companies will already have electronic or biometric systems installed and functioning, others might not, but identifying who is who ought to be relatively straightforward. Most companies will have their processes well documented with a unique reference number assigned to each process.

While these processes may well have been documented for a considerable period of time, it is important to recognise that they may have been defined before security formed part of the requirements. This should be recognised and appropriate steps taken to address this. Technology, too, should be simple enough, as each piece of technology, whether servers, desktop, or mobile device will have a unique asset number, and internet connectivity can be recorded via the unique media access control (MAC) address inside the hardware, as well as the internet protocol (IP) address used to connect to the network, whether from inside the company, or from outside the company via the internet.

Looking at systems next, each piece of technology will have an operating system, which will be identifiable. There will be one or more services running on the equipment, which will be identifiable, and there will be one or more applications running on the equipment, all of which will be identifiable. Where access to cloud systems is available, this will be either at a high level, such as SaaS or some service such as desktop as a service (DaaS), which can be identified. Equally, if the access is to a lower level of service such as PaaS or IaaS, this too can be identified. There may be multiple systems accessed, operated by multiple

providers, which may also involve brokers or other service providers, all of which can be identified.

This brings us to a more difficult area, the security properties. Confidentiality can be achieved by ensuring only the correctly authorised people can be granted access to confidential information. This can be achieved by proper access control, and monitoring. Integrity is slightly more challenging, as it is technically more challenging to ensure that information, once saved into a system has not been tampered with, particularly in the case of databases. This can be addressed by logging every change made to every transaction within a system, logging who made the change, when, from what location and so on. Thus each change in the information state can be preserved, which would allow recreation of the original if the change was malicious.

However, our requirement to address the new security properties of sustainability, resilience and ethics presents the biggest challenge. We could address sustainability of security by using redundancy to ensure continuity of operations in the event of some business disaster or major security breach. This may involve an element of lost time due to set up and configuration time needed to restore systems.

Resilience could be addressed by having a permanently running system mirror which allows for an extremely rapid recovery from unexpected shock. The additional costs of addressing sustainability and resilience would need to be considered. For business critical systems, the additional costs of ensuring sustainability and resilience may end up providing cheap insurance.

Ethics, which generally would include company approach to corporate social responsibility, could be addressed by viewing how suppliers approach these issues, usually disclosed in annual reports, corporate social responsibility reports or on the company website.

Clearly CSPs who concentrate on availability in their SLAs without considering accountability, assurance, audit, confidentiality, compliance, integrity, privacy, responsibility and security, thus leaving the cloud user to carry the can, might well be considered as irresponsible and unethical in their behaviour. The same might be said for companies who provide poor service in other areas, such as outsourced activities which might have an impact on security and privacy.

3.4 Addressing Two Critical Remaining Obstacles to Cloud Security

We would like to think that there are no weaknesses in the conceptual framework we have developed for cloud security assurance. But to do so would be naïve, as the framework has been necessarily developed to address all aspects of cloud security under the control of the company operating the framework. Unfortunately, the very mechanism of cloud computing means that not all areas are completely under the control of the company operating the framework. At least one or more companies involved in the cloud ecosystem will not be under the control of the company operating the framework, and this presents a key weakness.

Our proposed framework addresses all three areas of people, process and technology, yet is still not foolproof, and here are some of the main reasons for this: CSP SLA limitations, and unwillingness to change; The threat environment; Standards issues; Management reluctance to take security seriously. One of the most important of these is the SLA between the company and the CSP. It is no accident that the standard SLA offerings from the major CSPs focus on availability. Their business model is geared to providing availability as the main service performance measure to which they purport to be accountable.

Accountability, assurance, audit, confidentiality, compliance, integrity, privacy, responsibility and security do not feature in the standard SLA (Duncan and Whittington 2015b). It is important that companies recognise that this represents the current status. Any additional requirements must be negotiated directly with the CSP, although it is encouraging to note that following an EU pilot study (EU 2012), the EU Commission proposed new guidelines for a standard EU SLA (EU 2014).

Another key area to be considered is the magnitude of the threat environment. Companies are bound by legislation, sometimes regulation, the need to comply with standards, industry best practice and are accountable for their actions. Attackers have no such constraints. They have different agendas, different skills levels, capabilities and resources at their disposal. Between them all, they can attack 24/7, 365 days a year. They don't work to rule, go home at 5:00 pm, take weekends off or go on holiday, at least not until they have the cash, in which case there are plenty more happy to take their place. In addition to this, Kaspersky (2013) suggest that over 200,000 new malware threats are being developed globally every day.

We are concerned about developing proper metrics for the six security goals of our proposed security assurance model. This will not be a trivial exercise and clearly we cannot do justice to all these areas within the space of this chapter. Accordingly, we will address each of these areas individually during the next year as part of our ongoing research.

4 Can We Outsource Measurement and How Would We Do It?

Management guru Harrington (1999) once said "Measurement is the first step that leads to control and eventually to improvement. If you can't measure something, you can't understand it. If you can't understand it, you can't control it. If you can't control it, you can't improve it."

In considering whether we can outsource measurement and thinking about how we can do it, we look at Duncan and Whittington (2016) where the authors first consider the cloud audit problem, and how this can impact on our plan. We also consider in Duncan and Whittington (2016) how correct use of the audit trail can help us ensure that a good solution to this problem can be achieved.

In previous work (Duncan and Whittington 2015b) on enhancing cloud security and privacy, the authors addressed issues arising due to the cloud service

provider's (CSP)'s lack of accountability in the standard service level agreement (SLA). The authors discuss the importance of the role assurance plays, and the two main mechanisms used to achieve this, namely compliance and audit.

Before understanding how the use of cloud impacts on the audit process, and how it differs from conventional IT audit, we need to first understand what audit is, why we need to do it, who should be doing it and how it should be done. We must also understand what special difficulties the use of cloud brings to audit. We therefore revisit the authors' definition of audit.

The Oxford English Dictionary (OED) defines audit as (OED 1989): ("To make an official systematic examination of (accounts), so as to ascertain their accuracy") and requires outsiders who are deemed to be both objective and expert to form their own opinion of what is being audited and then to publicly state their confidence (or otherwise) in the reliability of what they have investigated. Auditing is not straightforward or easy. Just as with accounting auditors, objectivity is difficult when companies pay auditors directly and auditors would also like to be retained for the following year. Audit is also potentially very expensive if done well by the best experts in the field and there is a temptation to reduce the experts' role to one of advising, often writing checklists to be administered by qualified technicians.

We first consider the three main purposes of audit, who should be carrying it out, and how it should be done. First, the most widely understood of which is the statutory requirement for financial statements to be audited by an independent external auditor, which has been a cornerstone of confidence in global financial systems since auditing was introduced. It provides assurance that company managers have presented a "true and fair" view of a company's financial performance and position, underpinning the trust and obligation of stewardship between company management and the owners of the company, the shareholders.

A second purpose of audit is IT systems audit. Traditional audit approaches often involved treating IT systems as "black box" systems, meaning trust was placed in the IT systems, and looking at the functioning of the IT system was not considered part of the statutory audit. These audits are usually conducted by IT specialists, often in conjunction with accounting audit professionals to ensure the functioning of these systems are properly understood. However, these are not mandated under statute, and there is no requirement for an annual audit to be undertaken.

A third purpose of audit is compliance, either with regulations, or more often with standards. This is often undertaken to assure shareholders and other stakeholders that the company is using best practice in its operations. This is particularly the case in cloud computing, where systems are operated by third parties beyond the control of the cloud user. Currently, the difficulties associated with performing an adequate cloud audit present one of the key barriers to cloud adoption (Armbrust et al. 2010). Again, these audits are not mandated under statute, nor is there a requirement for an annual audit to be undertaken.

Clearly, in order to take an economic approach to providing a satisfactory level of service, utilising the first purpose of audit would not be appropriate, due

to the high costs involved. However, the second purpose of audit would provide a high level of assurance to cloud users if it were carried out on the monitoring system at the beginning of the contract. Thereafter, using the third purpose of audit could provide assurance in the long run that the outsourcing company is providing an adequate level of performance.

Having said that, there are some shortcomings with the cloud audit trail process, as discussed by (Duncan and Whittington 2016), which we would do well to take into account. The six security issues addressed in Duncan and Whittington (2015c) have been expanded to ten, with the addition of the following four security issues: measurement and monitoring; management attitude to security; security culture in the company; and the threat environment.

Since the Duncan and Whittington (2015e) paper already covered the measurement issue, this leaves the last three to consider. There is no doubt that management approach to security will have a major impact on how well a company can stand up to attack, and indeed this approach will also determine how good the security culture within the company will be. Our approach to solving these issues is to minimise the impact any adverse management approach is likely to have on security. Obviously, we have no control over the threat environment, our only approach being to make life as difficult as possible for attackers to gain access.

A fundamental element of the audit process is the audit trail, and having two disciplines involved in providing cloud audit services means there are two different disciplines to contend with, namely accounting professionals and security professionals. An obvious concern is what is meant by the term “audit trail”. It is easy to assume that everyone is talking about the same thing, but is that actually the case? To an accounting professional, the meaning of an audit trail is very clear.

The Oxford English Dictionary (OED) (OED 1989) has two useful definitions of an audit trail: “(a) Accounting: a means of verifying the detailed transactions underlying any item in an accounting record; (b) Computing: a record of the computing processes which have been applied to a particular set of source data, showing each stage of processing and allowing the original data to be reconstituted; a record of the transactions to which a database or a file has been subjected”. This suggests common understanding, but often this is not evident in computing research.

What is abundantly clear, both from an accounting and a computing security perspective, is that users should only be able to read the audit trail (Anderson 2008). While it is simple enough to restrict users to read-only access, this does not apply to the system administrators. This presents an issue where an intruder gets into a system, escalates privileges until root access is obtained, and is then free to manipulate, or delete the audit trail entries in order to cover their tracks.

A simple solution to this key problem would be for the outsourcing contractor to run the audit trail on their own systems, thus removing all vulnerabilities from the user’s system and ensuring continuity of monitoring and preservation of a full and proper audit trail.

Turning back to the questions of the chapter, we have now established the mechanics of how we might achieve this goal, meaning we have a viable methodology that can be used to achieve these goals. Thus we need to consider in which cases this methodology might be deployed. Whether or not they have the will, it is certainly the case that large corporates can afford the calibre of staff necessary to take care of these issues in-house.

However, in the case of small to medium sized enterprises (SME)s and micro enterprises (ME)s, these companies may well not have the resources to deploy an adequate calibre of staff to handle this challenging technical task. Equally, the management may not have sufficient knowledge to be able to define adequate and proper metrics to measure. This is likely to put such companies at a commercial disadvantage as compared to large corporates.

However, by providing them with an opportunity to have access to this service as an outsourced service, provided to a high standard, this will free them and their staff to concentrate on the areas of business which they are most skilled at. This should permit them to take comfort that a vital, and highly specialised, requirement needed to ensure the security of their business is being properly taken care of, while at the same time, removing some of the competitive disadvantage that they would otherwise suffer from.

5 Discussion

Pearson and Charlesworth (2009) argue that *accountability* may be a solution to the privacy problem in the cloud, but this may be true also in the general case if we can persuade providers that “doing the right thing” may be a business advantage (Jaatun et al. 2016). Incident response in the cloud is difficult for many reasons, not least because many cloud services are delivered as part of complex provider chains, and incidents that occur at one part of the chain may have implications at the other end (Jaatun and Tøndel 2015).

Some recent developments may provide additional incentives to an accountability-based approach. The European Data Protection Regulation (EDPR) (EU 2016), which will come into force by 2018, has specific provisions for data breach notification, which may encourage providers to use notification technology that is already available. However, it may be argued that being too open about incidents that have occurred in your system both could create bad publicity and allow your competitors (not to mention other attackers) too much insight into your weak spots (Frøystad et al. 2016).

Against this backdrop emerges a major selling point for outsourcing incident management services to a trusted third party. Cloud customers could ensure that their MSSP either covers the entire provider chain, or that the provider chain is covered by a set of MSSPs that collaborate. This avoids having to reveal “arbitrary” incident information to the next provider in the chain, instead sending it to the MSSP, who in this context would fill a similar role as an auditor. It is not a long stretch to imagine that such an MSSP also could do other forms of security-relevant measurements, either using agents or other mechanisms (Doelitzscher et al. 2013).

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 (Tøndel et al. 2014).

A customer that has security controls in place, trains its people, has implemented security awareness, and knows what the threats might be, gets more benefit from 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 manpower, 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. Moreover, 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. Ahmad et al. (2015) highlight the importance of learning from incidents, and the difficulties some experience with information sharing even within the same organization. Using professional third party could be a way to bridge this gap.

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. Organization B offers different types of SLAs 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 in a best effort manner, 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 (Schneier 2014). It is hard to state SLAs because there is no level of predictability in these kinds of situations.

Proper measurement and monitoring can not only provide an effective means of ensuring proper standards of security and privacy can be maintained on a day to day basis, but in addition, can provide effective compliance assurance to ensure cloud users can demonstrate a highly ethical approach to the stewardship of customers' data. Where the measurement and monitoring solution is added to the incident response solution, this can provide a repository of additional long term forensic material in the event of a cloud breach, as well as freeing internal company resources to address other important company issues.

6 Conclusion

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 from 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 descriptions at the provider's websites are unclear, and often confusing. Mapping those services to either the incident management model, or, e.g., the Observe-Orient-Decide-Act (OODA) decision-making life-cycle phases (Boyd 1987) 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.

We have looked at some of the challenges facing companies who seek to obtain good cloud security assurance. We have seen how weaknesses in standard CSP SLAs can impact on cloud security. We have identified issues with cloud security standards, and how that might impact on cloud security. We have considered how the lack of accountability can impact on security. We have briefly outlined how our cloud security assurance framework operates, and have discussed how the above issues must additionally be addressed.

In looking at measurement literature, we see how some aspects are quite mature and well understood, but that more modern methods of management such as sustainability, resilience and ethics present new challenges due to the dearth of research in these areas. In looking at how our framework operates, we have discussed how the best security approach needs to consider not just a technical solution, but must address people, process and technology.

We have touched on how these difficult areas of security might be approached as part of a comprehensive security solution based on our proposed framework. Clearly, companies could benefit from further research in several of these areas, and in particular, measurement. However, we would caution that action is needed now, not several years down the line when research reaches a more complete level of success in these areas. The threat environment is too dangerous. Companies have to act now to try to close the door, otherwise it may be too late.

Where a company is prepared to use an outsourced service for incident response, it is clear that there will be synergies to be gained by also using the same outsourced service to measure and monitor the effectiveness of the ongoing security position of the company as a whole. Our proposal will address one of the fundamental weaknesses of security monitoring, namely the lack of security which conventional systems impose on the audit trail, which will clearly provide a considerable improvement on the status quo.

Acknowledgements. The research in this paper has partly been supported by the European Commission (A4Cloud project, grant no. 317550).

References

- Ahmad, A., Maynard, S.B., Shanks, G.: A case analysis of information systems and security incident responses. *Int. J. Inf. Manag.* **35**(6), 717–723 (2015)
- Anderson, R.J.: *Security Engineering: A Guide to Building Dependable Distributed Systems*, vol. 50. Wiley, Hoboken (2008)
- Arjoon, S.: Corporate governance: an ethical perspective. *J. Bus. Ethics* **61**(4), 343–352 (2012)
- Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M.: A view of cloud computing. *Commun. ACM* **53**(4), 50–58 (2010)
- Baldwin, A., Beres, Y., Mont, M.C., Shiu, S., Duggan, G., Johnson, H., Middup, C.: An experiment in decision making WEIS 2011. In: WEIS, pp. 1–28 (2011)

- Beautement, A., Pym, D.: Structured systems economics for security management. In: WEIS, pp. 1–20 (2010)
- Boyd, J.R.: Organic design for command and control. A discourse on winning and losing (1987)
- Chang, V., Ramachandran, M., Yao, Y., Kuo, Y.H., Li, C.S.: A resiliency framework for an enterprise cloud. *Int. J. Inf. Manag.* **36**(1), 155–166 (2016)
- Chapin, F.S., Kofinas, G.P., Folke, C.: Principles of Ecosystem Stewardship: Resilience-Based Natural Resource Management in a Changing World. Springer, Heidelberg (2009)
- Doelitzscher, F., Ruebsamen, T., Karbe, T., Reich, C., Clarke, N.: Sun behind clouds - on automatic cloud security audits and a cloud audit policy language. *Int. J. Adv. Netw. Serv.* **6**(1&2) (2013)
- Duncan, B., Pym, D.J., Whittington, M.: Developing a conceptual framework for cloud security assurance. In: 2013 IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), Bristol, vol. 2, pp. 120–125. IEEE (2013)
- Duncan, B., Whittington, M.: Compliance with standards, assurance and audit: does this equal security? In: Proceedings of the 7th International Conference on Security of Information and Networks, Glasgow, pp. 77–84. ACM (2014)
- Duncan, B., Whittington, M.: Company management approaches stewardship or agency: which promotes better security in cloud ecosystems? In: Cloud Computing, Nice, pp. 154–159. IEEE (2015a)
- Duncan, B., Whittington, M.: Enhancing cloud security and privacy: broadening the service level agreement. In: The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2015), Helsinki, Finland, pp. 1088–1093 (2015b)
- Duncan, B., Whittington, M.: Information security in the cloud: should we be using a different approach? In: 2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom), Vancouver, pp. 1–6 (2015c)
- Duncan, B., Whittington, M.: Reflecting on whether checklists can tick the box for cloud security. In: Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom, Singapore, vol. 2015-February, pp. 805–810. IEEE (2015d)
- Duncan, B., Whittington, M.: The importance of proper measurement for a cloud security assurance model. In: 2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom), Vancouver, pp. 1–6 (2015e)
- Duncan, B., Whittington, M.: Enhancing cloud security and privacy: the power and the weakness of the audit trail. In: Submitted to Cloud Computing, Rome, pp. 1–6. IEEE (2016)
- EU: Unleashing the Potential of Cloud Computing in Europe (2012)
- EU: Cloud service level agreement standardisation guidelines. Technical report, EU Commission, Brussels (2014)
- EU: Reform of EU data protection rules (2016)
- Frøystad, C., Gjære, E.A., Tøndel, I.A., Jaatun, M.G.: Security incident information exchange for cloud services. In: Proceedings of International Conference on Internet of Things and Big Data (2016)
- Gill, A.: Corporate governance as social responsibility: a research agenda. *Berkeley J. Int. Law* **26**(2), 452–478 (2008)
- Harrington, H.J.: Measurement. CIO, 19 September 1999
- Huse, M.: Accountability and creating accountability: a framework for exploring behavioural perspectives of corporate governance. *Br. J. Manag.* **16**(S1), S65–S79 (2005)

- Ioannidis, C., Pym, D., Williams, J.: Sustainability in information stewardship: time preferences: externalities and social co-ordination. In: WEIS 2013, pp. 1–24 (2013)
- Jaatun, M.G., Nyre, Å.A., Alapnes, S., Zhao, G.: 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)
- Jaatun, M.G., Pearson, S., Gittler, F., Leenes, R., Niezen, M.: Enhancing accountability in the cloud. *Int. J. Inf. Manag.* (2016, to appear)
- Jaatun, M.G., Tøndel, I.A.: How much cloud can you handle? In: 2015 10th International Conference on Availability, Reliability and Security (ARES), pp. 467–473 (2015)
- Kao, R.: Stewardship Based Economics. World Scientific, Singapore (2007)
- Kaspersky: Global Corporate IT Security Risks. Technical report, May 2013
- Kolk, A.: Sustainability, accountability and corporate governance: exploring multinationals’ reporting practices. *Bus. Strateg. Environ.* **17**(1), 1–15 (2008)
- Neumann, P.G.: Computer-Related Risks. Addison-Wesley, Reading (1995)
- OED: Oxford English Dictionary (1989)
- Pallas, F.: An agency perspective to cloud computing. In: Altmann, J., Vanmechelen, K., Rana, O.F. (eds.) GECON 2014. LNCS, vol. 8914, pp. 36–51. Springer, Heidelberg (2014). doi:[10.1007/978-3-319-14609-6_3](https://doi.org/10.1007/978-3-319-14609-6_3)
- Parker, D.B., Crime, F.C.: Fighting Computer Crime: A New Framework for Protecting Information. Wiley, Hoboken (1998)
- Pearson, S., Charlesworth, A.: Accountability as a way forward for privacy protection in the cloud. In: Jaatun, M.G., Zhao, G., Rong, C. (eds.) CloudCom 2009. LNCS, vol. 5931, pp. 131–144. Springer, Heidelberg (2009). doi:[10.1007/978-3-642-10665-1_12](https://doi.org/10.1007/978-3-642-10665-1_12)
- PWC: UK Information Security Breaches Survey. Technical report, London, April 2012
- Reyes, A.: Outsourced incident management services (2015)
- Reyes, A., Jaatun, M.G.: Passing the buck: outsourcing incident response management. In: IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom), pp. 503–508 (2015)
- Schneier, B.: The future of incident response. *IEEE Secur. Priv.* **12**(5), 96–96 (2014)
- Tøndel, I.A., Line, M.B., Jaatun, M.G.: Information security incident management: current practice as reported in the literature. *Comput. Secur.* **45**, 42–57 (2014)
- Willingmyre, G.T.: Standards at the crossroads. *StandardView* **5**(4), 190–194 (1997)

Enterprise Security

Second International Workshop, ES 2015, Vancouver,
BC, Canada, November 30 – December 3, 2015, Revised
Selected Papers

Chang, V.; Ramachandran, M.; Walters, R.J.; Wills, G.
(Eds.)

2017, X, 277 p. 64 illus., Softcover

ISBN: 978-3-319-54379-6