



University
of Glasgow

Grispos, G., Glisson, W.B., and Storer, T. (2013) *Cloud security challenges: Investigating policies, standards, and guidelines in a Fortune 500 organization*. In: 21st European Conference on Information Systems, 5-8 Jun 2013, Utrecht, The Netherlands.

Copyright © 2013 The Authors

A copy can be downloaded for personal non-commercial research or study, without prior permission or charge

The content must not be changed in any way or reproduced in any format or medium without the formal permission of the copyright holder(s)

<http://eprints.gla.ac.uk/76290/>

Deposited on: 16 August 2013

Cloud Security Challenges: Investigating Policies, Standards, and Guidelines in a Fortune 500 Organization

George Grispos, School of Computing Science, University of Glasgow, Glasgow, United Kingdom, g.grispos.1@research.gla.ac.uk

William Bradley Glisson, Humanities Advanced Technology and Information Institute, University of Glasgow, Glasgow, United Kingdom, Brad.Glisson@glasgow.ac.uk

Tim Storer, School of Computing Science, University of Glasgow, Glasgow, United Kingdom, timothy.storer@glasgow.ac.uk

Abstract¹

Cloud computing is quickly becoming pervasive in today's globally integrated networks. The cloud offers organizations opportunities to potentially deploy software and data solutions that are accessible through numerous mechanisms, in a multitude of settings, at a reduced cost with increased reliability and scalability. The increasingly pervasive and ubiquitous nature of the cloud creates an environment that is potentially conducive to security risks. While previous discussions have focused on security and privacy issues in the cloud from the end-users perspective, minimal empirical research has been conducted from the perspective of a corporate environment case study. This paper presents the results of an initial case study identifying real-world information security documentation issues for a Global Fortune 500 organization, should the organization decide to implement cloud computing services in the future. The paper demonstrates the importance of auditing policies, standards and guidelines applicable to cloud computing environments along with highlighting potential corporate concerns. The results from this case study has revealed that from the 1123 'relevant' statements found in the organization's security documentation, 175 statements were considered to be 'inadequate' for cloud computing. Furthermore, the paper provides a foundation for future analysis and research regarding implementation concerns for corporate cloud computing applications and services.

Keywords: Cloud Computing, Information Security, Corporate Policy, Requirements, Standard, Guidelines

1. Introduction

Cloud computing is rapidly becoming pervasive in today's globally integrated networks. This emerging paradigm allows an organization to reduce costs and develop more reliable and highly scalable solutions [1]. There is an apparent consensus that cloud computing is increasingly integrating into the business environment [2, 3]. The 2011 Ernst and Young Global Information Security Survey [3] reported that 36% of respondents were currently using cloud computing services, as compared to 23% from the previous year. Furthermore, this report goes on to state that 25% of respondents are currently evaluating or investigating the use of cloud services in the subsequent year. In concert with these findings, the AMD Global Cloud Computing Study [2] reported that 37% of surveyed businesses globally are deploying applications or storing data in cloud environments. Cloud computing services are also being utilized by governments in an attempt to reduce costs and improve the efficiency of IT

¹Please cite this paper as: Grispos, G., Glisson, W.B., and Storer, T. (2013) *Cloud Security Challenges: Investigating Policies, Standards, and Guidelines in a Fortune 500 Organization*. In: 21st European Conference on Information Systems, 5-8 Jun 2013, Utrecht, The Netherlands.

solutions within their agencies [4]. The United States Federal Government is expected to save \$10 billion in IT costs by migrating government services to cloud computing [5].

Although the benefits of cloud computing are attractive, a major concern is the security of data and applications in these environments. This apprehension focuses on data confidentiality and auditability, data lock-in, a lack of encryption, the impact of borderless and virtualized environments, as well as cloud providers not addressing requirements from a business, information technology or security perspective [1, 3]. These fears are being validated as cloud adopters witness an increase in the number of cloud infrastructure security incidents as compared to traditional IT infrastructure security events [6]. The real-world impact is that security incidents and data breaches can have financial consequences on a corporate organization [7]. The Ponemon Institute [8] indicates that although the cost of data breaches has declined in the past year, data breaches are still reported to have cost British and German organizations on average between \$2.7 million and \$4.4 million. In addition to economic losses, security incidents and data breaches can result in a loss of customers, damaged reputations, delayed software releases and a reduction in investor confidence [7]. To reduce the likelihood and impact of security incidents and data breaches, organizations implement information security programs [9]. The primary objective of an information security program is to protect the integrity, confidentiality and availability of information and applications while ensuring that legal and regulatory requirements are also fulfilled [9, 10]. Hence, an organization's overall strategy towards specific environments like private and public clouds should be reflected in their policies, standards and guidelines. Although the European Network and Information Security Agency [11] and the Cloud Security Alliance [12] have defined security documentation for cloud computing environments, very little research investigates the application of this documentation towards mitigating cloud-related security incidents and data breaches.

This research presents an empirical case study investigating information security policies, standards, and guidelines in a Global Fortune 500 organization. The research begins to identify potential areas of information security documentation exposure from the perspective of a large organization through the examination of 164 policies, 1,255 standards and 674 guidelines. The research contribution is an empirical report identifying security issues along with research opportunities in policies, guidelines and procedures in large organizations that are considering migrating to a public cloud environment. The structure of the paper is as follows. Section 2 presents an overview of cloud computing security challenges and issues identified from the literature, Section 3 defines the method of data collection implemented in this study. Section 4 provides insight into the organization through an analysis of existing documentation and identifies current enhancement opportunities. Section 5 draws conclusions from the work conducted and presents ideas for further work.

2. Analysis of Cloud Security Issues

Cloud computing has been defined as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [13]. Grispos et al., [14] have discussed the different service and deployment configuration options of a cloud computing environment from an information security perspective.

The security of data and applications is a concern for organizations wishing to adopt cloud computing services. Armbrust et al., [1] cite a number of security concerns regarding cloud adoption including data confidentiality and auditability, business continuity and data lock-in. Subashini & Kavitha [15] highlighted security issues applicable to various layers of the cloud computing environment while noting that security needs will vary for each delivery model. The Cloud Security Alliance (CSA) has also identified several critical areas in cloud environments [12]. The high-level domains along with associated research in those areas are available in Table 1 – Cloud Security Research. Initial areas of interest are unauthorized data access, vendor lock-in, legal issues and virtualization.

One of the biggest concerns for an organization, considering the adoption of cloud computing, is preventing unauthorized access to data resources [16]. This is a concern because an organization's traditional authentication and authorization framework does not naturally extend into the cloud environment and requires modification to support cloud computing services [17]. This problem is particularly evident in Software-as-a-Service (SaaS) environments, where a user's credentials are likely to be stored in the SaaS providers' databases, and who effectively become responsible for security and access control mechanisms [18]. Having different authentication systems for internal and cloud-based resources is likely to further complicate the issue and become impractical over time [16]. One proposed solution is the use of a federated identity management system, allowing users to access the cloud environment from anywhere outside the traditional workplace while authentication credentials remain within the corporate boundary [19]. Additionally, Kaufman [20] suggests that to ensure data confidentiality, integrity, and availability, cloud providers must offer capabilities that include the encryption of data across their entire infrastructure and a backup mechanism to replace corrupted data. A regular backup mechanism can ensure a quick recovery of service in the case of disaster or accidental data loss [17, 21]. The Data Protection Working Party [22] recommends that organizations utilizing cloud services instruct cloud providers to only store applications, primary and backup data in pre-defined physical locations. The storage of data in known physical locations also supports compliance with regulatory and jurisdictional requirements [12, 22].

Another concern is that migration from one cloud provider to another can lead to issues like data remembrance and vendor lock-in [12, 23]. Currently, immediate compliance with a customer's request to comprehensively destroy data from the provider's infrastructure is uncertain [23]. For example, Google's policy is that once data is deleted, it is removed from all active and replication servers. However, the data is only completely removed when it is overwritten by another customer's data over a period of time [24]. This brings up an interesting question. When a customer decides that they would like to leave a service, what confirmation can cloud providers offer to verify that all of the user's data has been completely erased from their storage facility? Moyle [25] has hypothesized that cloud service providers will restrict their customers logical access to their physical data through a number of 'security controls'. As a result, this can lead to the phenomenon referred to as 'vendor lock-in' [23]. Vendor lock-in can inhibit an organization from migrating from one provider to another [1, 12]. This environment can also be encouraged through the implementation of proprietary or non-standard Application Programming Interfaces (APIs) and data storage methods.

Large organizations are often familiar with legislative compliance requirements for logging system activity. Often legal and regulatory requirements such as the Sarbanes-Oxley (SOX) Act of 2002 and the Health Insurance Portability and Accountability Act (HIPAA) of 1996 require that an accurate time source is used to synchronize the system clocks of any potential logs [26]. The challenge arises in the cloud environment where data and log files are stored in more than one geographical location and possibly located in different time zones. Cloud providers need to ensure that a universal time source is used across its infrastructure to eliminate potential discrepancies in timestamps [12]. Further challenges identified include provisions on how long logs must be maintained by the cloud provider, where the cloud provider can store logs, who will be responsible for the creation and maintenance of the logs, what security controls must be in place to prevent unauthorized modification, as well as under what conditions the logs can be deleted [27-29].

Virtualization is also expected to present a number of security challenges in cloud environments [16, 30-33]. Ibrahim, et al., [31] discussed how known security issues, within virtualized environments, can also be found in the various components of an Infrastructure-as-a-Service (IaaS) implementation. This issue is further enhanced in a multi-tenancy virtual machine-based infrastructure where, in the event malicious code is inserted into the virtualization layer, an attacker can gain full control over the physical infrastructure and all the virtual machines connected to that particular infrastructure [16, 30]. Ristenpart et al., [32] have successfully demonstrated that this practice is a security concern for both the cloud provider and the organizations using the resulting service. They demonstrated how cross-virtual machine attacks can result in data leakage between virtual machines which share the same

physical resources in the Amazon EC2 Cloud [32]. Complicating matters, Wei, et al., [33] described how an attacker can modify virtual machine images hosted in the cloud. These virtual machine images are used to create virtual machine instances which could be used to allow an attacker to access the virtual machine, data, applications and execute malicious code [33].

CSA Domain Name	Cite(s)
Governance and Enterprise Risk Management	[20, 28, 34, 35]
Legal Issues: Contracts and Electronic Discovery	[14, 15, 36-38]
Compliance and Audit Management	[1, 15, 20, 34, 39]
Information Management and Data Security	[15-17, 20, 40, 41]
Interoperability and Portability	[17, 23, 40]
Traditional Security, Business Continuity and Disaster Recovery	[15, 34, 40]
Data Centre Operations	[12, 28]
Incident Response	[14, 36, 42, 43]
Application Security	[17, 20, 34, 40, 41]
Encryption and Key Management	[12, 39]
Identity, Entitlement and Access Management	[15-17, 41]
Virtualization	[16, 24, 32, 33, 44]

Table 1 - Cloud Security Research

Cloud security is a multi-faceted environment that consists of the provider, the user, and any other third-party vendor who provides security software and services to either the provider or the user [40]. Research has focused on a number of security issues in cloud computing environments. However, very little empirical research has been conducted to examine real-world information security documentation in an organization assessing cloud computing ‘security-readiness’.

3. Method

Based on growing industry interest in cloud computing environments, it was hypothesized that current information security documents are potentially putting organizations at risk. Hence, this research empirically investigates security-readiness through exploratory interviews and an examination of information security documents relevant to cloud computing environments. Exploratory case studies provide insight into understanding real-world problems and context along with identifying future areas of research [45]. The case study was completed between May and August 2012 and focuses on the information security documentation implemented in a Global Fortune 500 organization. In order to attain accurate information and foster an environment where all parties are comfortable presenting commercially sensitive information, the name of the organization is being withheld to ensure organizational anonymity. Hence, the names of the documents, security processes and groups have all

been altered and the results of the exploratory interviews conducted with employees are presented anonymously.

An analysis of the existing literature was conducted to identify and develop a broad understanding of the major themes regarding information security concerns in the cloud. The literature was collected from a number of sources including academic papers from online collections, industrial whitepapers and relevant textbooks. For the purpose of this discussion, the authors highlight five domains from the Cloud Security Alliance report [12] and relevant literature. These domains include: Information Management and Data Security, Interoperability and Portability, Incident Response, Encryption and Key Management, and Virtualization.

In order to acquire an understanding of the Global Fortune 500 organization's context, exploratory interviews were conducted with four senior members of the organization's security team. These senior members included: two security analysts, an enterprise security architect and an IT security manager. The security team is responsible for enforcing security controls during the application development process, as well as implementing everyday operational security. The purpose of the exploratory interviews was to identify the high-level information security documentation containers used within the organization and to investigate what security documents are applied to various projects. Each interview lasted 45 minutes and the interviewee's responses were recorded by hand. All hand-written notes were digitally recorded approximately within one hour after the interview was completed. The security documentation containers identified in the interviews are as follows:

- The *Technology Risk Repository (TRR)* contains documentation describing appropriate communication within the organization. These documents specify that all confidential or sensitive information must be encrypted, the identity of recipients of confidential or sensitive information must be verified and that all devices must be monitored for inappropriate use.
- The *Information Security Repository (ISR)* contains documentation providing high-level requirements regarding the organization's policy framework and compliance infrastructure. This includes information pertaining to communications and operations management, specific cryptographic algorithms, incident management procedures and business continuity requirements.
- The *Risk Management Repository (RMR)* contains documentation which defines how the organization communicates with external contractors, customers and regulators. It also contains policies to ensure compliance with legal and regulatory requirements.

For the purpose of this research, three main types of security documents were identified from the repositories: policies, guidelines and standards. The objective of an information security policy is to define "what" is to be done, while standards and guidelines specify "how" the policy objectives will be implemented [9, 46]. Information security policy statements define "the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations" and are high-level statements which are technology and solution-independent documentation [9, 47]. Standards and guidelines provide detailed information enabling employees to achieve objectives stated in security policies [48]. The literature review was used as a filtering guide to identify areas that present cloud security issues.

4. Security Documentation Analysis

A total of 127 security documents containing 2,093 security-related statements were available for examination. The Technology Risk Repository (TRR) consisted of 89 security documents containing 1,268 statements. The Information Security Repository (ISR) contained 14 security documents containing 232 statements. The Risk Management Repository (RMR) consisted of 24 security documents containing 593 statements. Statements within the various security documents were categorized as either 'relevant', 'non-relevant' or 'further research required'. A 'relevant' classification is one which, in its current format, is applicable to cloud computing environments. For example, a statement like 'cryptography mechanisms must be utilized to achieve data integrity and

confidentiality’ would also apply to any potential cloud computing service used by the organization. A ‘non-relevant’ classification is one which is not applicable to cloud computing environments. An example of such a statement is a ‘clear desk’ policy which dictates that all employees must not leave sensitive information on their desks overnight. A classification of ‘further research required’ indicates that there is the potential for the statement to be relevant but additional investigations are required. Such an example would be specific server-side configurations for UNIX and Windows networked machines. This is due to the fact that it is not clear if the specific configurations will be applicable to, or can be implemented in, cloud-based instances. This information is available in Table 2 - Repository Analysis.

Document Name/Repository	TRR	ISR	RMR	Total
<i>Total Policy Documents</i>	56	5	0	61
<i>Total Policy Statements</i>	56	108	0	164
<i>Relevant Policy Statements</i>	34	81	0	115
<i>Non- Relevant Policy Statements</i>	22	27	0	49
<i>Require Further Research Policy Statements</i>	0	0	0	0
<i>Total Standard Documents</i>	27	4	0	31
<i>Total Standard Statements</i>	1194	61	0	1255
<i>Relevant Standard Statements</i>	595	28	0	623
<i>Non- Relevant Standard Statements</i>	101	33	0	134
<i>Require Further Research Standard Statements</i>	498	0	0	498
<i>Total Guideline Documents</i>	6	5	24	35
<i>Total Guideline Statements</i>	18	63	593	674
<i>Relevant Guideline Statements</i>	1	62	322	385
<i>Non- Relevant Guideline Statements</i>	17	1	24	42
<i>Require Further Research Guideline Statements</i>	0	0	247	247

Table 2 - Repository Analysis

Additional analysis categorized ‘relevant’ statements as being ‘adequate’ or ‘inadequate’. An ‘adequate’ statement addresses cloud security risks for any potential cloud computing services used by the organization. For example, a statement like ‘all legal and regulatory requirements must be considered when storing personal data’ would be considered as an ‘adequate’ statement. An ‘inadequate’ statement does not mitigate cloud security risks. An example of such a statement is ‘all virtual machine instances must be locked down using the VMware Lockdown Standard. This statement was considered ‘inadequate’ as the standard assumes the analyst ‘locking down’ the virtual machine has control over the hypervisor. This assumption could be invalid in a public cloud environment. From the 115 ‘relevant’ policy statements, eight were considered to be ‘inadequate’ for cloud computing. Out of the 623 ‘relevant’ standard statements, 61 were considered to be ‘inadequate’ for cloud computing. Finally, from the ‘relevant’ 385 guideline statements, 106 were considered to be ‘inadequate’ for cloud computing. This information is summarized in Table 3 - Relevant Analysis. The results indicate that opportunities exist within the organization to improve security documents related to Interoperability and Portability, Information Management and Data Security, Incident Response, Encryption and Key Management, and Virtualization.

4.1 Interoperability and Portability

The organization currently does not have a process to govern a migration from one cloud provider to another or a process to govern how to completely remove its data and applications from the infrastructure of a legacy provider after a migration. This lack of a policy process could lead to eventual vendor lock-in. This process would need to define requirements for cloud providers to ensure they are able to guarantee that data migrated from the legacy provider to a new provider is done so in a

suitable and readable format. When selecting a cloud provider, the organization must also ensure that the application programming interfaces (APIs) used by the cloud provider are either non-proprietary or the provider can guarantee that data or application utilizing these interfaces can be easily migrated or removed from its infrastructure. Additionally, organizations should ensure that virtual machine instances and virtual machine images are also stored in a format which can allow them to be easily migrated between providers, for example the Open Virtualization Format (OVF) [12]. Any future cloud migration process should also define how logs, metadata and backups of data will be migrated from one provider to another. Will the legacy cloud provider perform the physical migration or will the organization need to handle this issue?

Document Name/Repository	TRR	ISR	RMR	Total
<i>Total Policy Statements</i>	56	108	0	164
<i>Relevant Policy Statements</i>	34	81	0	115
<i>Adequate Policy Statements</i>	28	79	0	107
<i>Inadequate Policy Statements</i>	6	2	0	8
<i>Total Standard Statements</i>	1194	61	0	1255
<i>Relevant Standard Statements</i>	595	28	0	623
<i>Adequate Standard Statements</i>	537	25	0	562
<i>Inadequate Standard Statements</i>	58	3	0	61
<i>Total Guideline Statements</i>	18	63	593	674
<i>Relevant Guideline Statements</i>	1	62	322	385
<i>Adequate Guideline Statements</i>	1	53	225	279
<i>Inadequate Guideline Statements</i>	0	9	97	106

Table 3 - Relevant Statements Analysis

4.2 Information Management and Data Security

The Identity Lifecycle Management process document defines the minimum security requirements for the identity lifecycle management processes used in the organization. The purpose of this document is to minimize the potential impact from intentional and unintentional unauthorized access to any of the organization's information resources. The document does not specifically address provisions on how cloud computing will integrate into the organization's current identity management (IdM) process. It does however state a formal process for establishing federated requests from third-party organizations. This third-party process specifies that the appropriate legal, regulatory and cryptographic controls must be in place and that the federating third-party complies with the organization's security policies. The process would be more comprehensive if it included details on the implementation of IdM for Software-as-a-Service (SaaS) applications in the cloud. If the organization performs a security assessment of a cloud provider, security analysts will need to establish how the provider intends to implement IdM. The third-party security assessment documents do not currently request this information. Hence, these documents need to be extended to include such provisions. This would allow the organization to identify the type of IdM solution the provider currently implements and to establish if this solution can be integrated with the organization's current IdM framework.

Documentation within the organization requires third-parties to have controls in place to ensure continuous availability of data which includes performing regular backups. Specific guidelines assume that a cloud provider will be responsible for providing backups. This requirement should be established on a case-by-case basis, as some cloud providers do not provide a full backup facility as part of their Service Level Agreement (SLA). For example, Amazon [49] does not currently provide this service in their SLA. The organization would benefit by establishing a cloud-based backup standard, which would clearly define where backup data can be stored, ensuring that the backup is encrypted and performed on a regular basis, as well as ensuring legal and regulatory compliance.

After considering regulatory obligations regarding data retention, current documentation requires that a secure and effective decommissioning process must be defined and implemented into all projects. The methods described in the documents include data-wiping storage media and physically destroying hardware components. This is a potential issue for a cloud-based service for multiple reasons. First, the methods may not be effective in a cloud-based environment or desired by the provider. Second, organizations are unlikely to have access to the physical hardware. Hence, the organization will need to establish with the cloud provider appropriate methods and assurances for the decommissioning of data, retention times and protocols when data breaches occur. These assurances will need to include all infrastructure components along with previous file versions, temporary files and even file fragments.

Ensuring continuous legal and regulatory compliance is a fundamental component of an organization's information security policy [50]. One such example is ensuring compliance with the Data Protection Directive when processing or storing personal data is undertaken [51]. The Directive clearly states that all personal data must be stored inside the European Union (EU) or in 'countries with an adequate level of protection' [51]. To comply with this requirement the organization currently requires that all personal data must be processed within the EU, unless the organization says otherwise. Cloud computing security statements need to be written to include log files, backups conducted by the cloud provider and any other metadata that could be used in incident management for regulatory purposes. Furthermore, the organization should include a security requirement for cloud providers to be able to provide both the logical and physical location of any of the organization's data stored in the provider's infrastructure.

4.3 Incident Response

Several security policies and standards targeted the detection and management of security incidents along with subsequent forensic investigations. These documents were created to address investigations involving traditional devices such as servers and personal computers. However, they did not take into consideration cloud computing environments. For example, a policy statement requires that a security analyst begins a chain of custody² for any electronic device seized that is suspected to be relevant to an investigation. This is generally an accepted practice in the forensic community [52]. The policy goes on to define how the suspected electronic device can be isolated and disconnected from its power source, allowing the security analyst to seize the device and begin the chain of custody. Creating a chain of custody for cloud computing investigations is anticipated to be more challenging [14, 36]. With data and applications being held by third parties, it is feasible that a chain of custody could be instigated by the cloud provider on behalf of an organization [14]. Due to the plausibility of this scenario, documentation would need to be developed to account for and address appropriate procedures for the creation and management of a chain of custody for cloud environments.

Another potential issue is that the documented forensic imaging methods may be insufficient in cloud environments [14, 36]. Traditionally, a byte-for-byte copy of the entire storage device is made, which is then used for analysis at a later stage [14]. The collection of evidence from cloud environments is unlikely to be straightforward and the tools currently used by the organization to collect potential evidence need to be investigated to determine their effectiveness in a cloud environment. Therefore, the organization needs to develop processes and guidelines to define evidence collection in cloud computing investigations. Documentation will also need to specify what evidence will be collected from cloud services [53]. This will require the creation of provisions to ensure that provider and application logs, along with any other relevant data, are handled appropriately. It is also plausible for organizations to mandate an accurate synchronization of timestamps to aid in the investigation of a security incident.

² A chain of custody provides a documented history, which should describe how evidence was collected, analysed and preserved in order to be presented as evidence in court (Vacca, 2005).

4.4 Encryption and Key Management

Current policies specify that, depending on data classification and regulatory requirements, encryption must be used to achieve data integrity and confidentiality. Policies and guidelines within the ISR define which encryption algorithms and key management processes must be implemented inside the organization. However, what happens when these services are needed outside of the organization? The documents referencing key management need to be expanded to specifically address who is responsible for encryption in a cloud environment. Is this the responsibility of the cloud provider? Regardless of the decision, standards will need to define how encryption keys will be managed between the two entities. Will the cryptographic keys be stored in the cloud itself? Who will have control of the cryptographic keys? One scenario is that policies will require that the organization retain all cryptographic keys within their possession. The drawback to this solution is that it limits the investigative support that is available from the cloud provider. Another issue to take into consideration is the possibility that cloud providers could store its data in countries where authorities have the legal right to request the cryptographic keys from all parties.

4.5 Virtualization

The only current documentation which specifically addresses virtualization is a lock-down standard for VMware virtual machines. The organization would need to address three main issues related to virtualization in cloud environments: ‘locking down’ cloud-based virtual machine instances, mitigating risks from hypervisor-level and cross-virtualization attacks, and virtual machine image security management. The current lock-down document for VMware virtual machines assumes that the administrator enforcing the ‘lockdown’ has physical access to the virtual machine at the hypervisor level. The standard statements in this document are unlikely to be plausible for a cloud virtual machine instance where the hypervisor is likely to be controlled by the cloud provider. Therefore, an alternative standard needs to be developed to ensure that a virtual machine instance in the cloud is ‘locked down’ and ‘hardened’ using policies more suitable for a cloud-based hypervisor. This standard would need to take into consideration the implementation of firewalls for inbound and outbound connections, as well as restrictions on Internet Protocol (IP) addresses for certain levels of access. In addition, this standard would also need to require that the physical machine hosting the hypervisor and virtual machine instance is also ‘locked down’. Security controls for applications and data connected to these virtual machine instances also need to be considered and defined.

Security guidelines are also needed to address and mitigate risks associated with hypervisor-level attacks including cross-virtualization attacks [32]. An insecure hypervisor can allow a malicious user to gain access to data stored in virtual machines hosted on a vulnerable hypervisor [32]. Therefore, subsequent requirements need to consider the use of cryptography and isolation as a solution to securing a hypervisor as well as implementing the principle of least privilege [44, 54]. Standards and guidelines will also need to specify how the organization manages a Virtual Machine Image (VMI) [54]. Wei et al., [33] suggest that a framework is developed to manage VMI creation, storage and destruction procedures. This framework is likely to contain controls such as filters to remove sensitive information from an image prior to publishing and a mechanism to track changes performed on a specific image to mitigate malicious image modification [33]. The organization should also ensure that requirements define the secure destruction of decommissioned VMIs.

5. Further Work and Conclusions

The increasing popularity of cloud computing services coupled with a growing threat from cyber-criminals creates an environment where security concerns have become a paramount issue. The results of this exploratory case study highlight not only the security issues that are being researched, but also identified opportunities to expand and develop information security documentation. This exploratory

research supports the idea that current organizational security policies are potentially putting organizations at risk. It hopefully encourages organizations interested in migrating to the cloud to perform a thorough examination of their security policies, standards and guidelines in reference to cloud environments.

This research presents a foundation for continued examination of cloud security documentation in corporate environments while generating technical and procedural ideas for mitigating future exposure. Future work in this area needs to examine the cloud computing application development process, the policies identified for further research and the technical aspects associated with conducting forensic investigations in cloud environments. Research needs to be expanded to examine the most effective way to integrate security into a cloud computing application development process. Research within the organization should conduct a more in-depth examination of the documents and statements that were identified as 'further research required'. Do the technical aspects of these documents and statements present potential security issues for the organization in a cloud environment? Do the organization's current service-level agreements sufficiently protect intellectual property that has been out-sourced to cloud-based service providers? The technical aspects of the tools used to conduct forensic investigations in the cloud need to be investigated. Do the tools that are currently available capture enough data? Ultimately, the case study needs to be expanded to multiple organizations in a variety of industries. The results from an expanded study would provide insight into common problems and encourage research focusing on real-world global solutions. Furthermore, the case study can be repeated in an organization which has already implemented cloud computing. The objective of this new case study would be to determine if the documentation issues identified in the studied organization are actually addressed when a cloud computing environment is implemented.

6. Acknowledgments

This work was supported by the A.G. Leventis Foundation. Any opinions, findings, conclusions or recommendations expressed in this paper are those of the authors and do not reflect the views of the A.G. Leventis Foundation. The authors would also like thank the Fortune 500 Organization for their support and feedback in this research

7. References

- [1] Armbrust, M., A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, *Above the Clouds: A Berkeley View of Cloud Computing*, in *University of California, Berkeley, Technical Report No. UCB/EECS-2009-28*. 2009.
- [2] AMD, *Adoption, Approaches & Attitudes The Future of Cloud Computing in the Public and Private Sectors - A Global Cloud Computing Study*. 2011.
- [3] Ernst & Young Advisory Services, *Into The Cloud, Out Of The Fog - The 2011 Global Information Security Survey*. 2011, Ernst & Young.
- [4] Wyld, D.C., *Moving to the Cloud: An Introduction to Cloud Computing in Government*. 2009, IBM Center for the Business of Government.
- [5] Bucci, S.P., *Getting Cyber Serious: Mastering the Challenges of Federal Cloud Computing*, in *Backgrounder*. 2012, The Heritage Foundation.
- [6] Trend Micro, *Cloud Security Survey Global Executive Summary*. 2011.
- [7] Glisson, W.B., A. McDonald, and R. Welland, *Web engineering security: a practitioner's perspective*, in *Proceedings of the 6th international conference on Web engineering*. 2006, ACM: Palo Alto, California, USA. p. 257-264.
- [8] Ponemon Institute LLC, *The 2011 Cost of Data Breach Study: Global*. 2012, Symantec.
- [9] Hansche, S., *Official (Isc)2 Guide to the Cissp Exam*. 2003, Florida: Auerbach Publishers Inc.
- [10] Diver, S., *Information Security Policy – A Development Guide for Large and Small Companies*. 2007, SANS Institute.

- [11] European Network and Information Security Agency, *Cloud Computing - Benefits, risks and recommendations for information security* 2009, ENISA.
- [12] Cloud Security Alliance, *Security Guidance for. Critical Areas of Focus in Cloud Computing*. 2011.
- [13] Mell, P. and T. Grance, *The NIST Definition of Cloud Computing - Special Pub: 800-145*. 2011.
- [14] Grispos, G., T. Storer, and W.B. Glisson, *Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics*. International Journal of Digital Crime and Forensics, 2012. **4**(2): p. 28-48.
- [15] Subashini, S. and V. Kavitha, *A survey on security issues in service delivery models of cloud computing*. Journal of Network and Computer Applications, 2011. **34**(1): p. 1-11.
- [16] Jansen, W.A., *Cloud Hooks: Security and Privacy Issues in Cloud Computing*, in *System Sciences (HICSS), 2011 44th Hawaii International Conference on*. 2011. p. 1-10.
- [17] Chow, R., P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, *Controlling data in the cloud: outsourcing computation without outsourcing control*, in *Proceedings of the 2009 ACM workshop on Cloud computing security*. 2009, ACM: Chicago, Illinois, USA. p. 85-90.
- [18] Janssen, M. and A. Joha, *Challenges for Adopting Cloud-based Software as a Service (SaaS) in the Public Sector*, in *ECIS 2011 Proceedings*. 2011.
- [19] Takabi, H., J.B.D. Joshi, and G. Ahn, *Security and Privacy Challenges in Cloud Computing Environments*. Security & Privacy, IEEE, 2010. **8**(6): p. 24-31.
- [20] Kaufman, L.M., *Data Security in the World of Cloud Computing*. Security & Privacy, 7(4), 61-64, 2009.
- [21] Sundararajan, S., H. Narayanan, V. Pavithran, K. Vorungati, and K. Achuthan, *Preventing Insider Attacks in the Cloud*. Communications in Computer and Information Science, 2011. **190**: p. 488-500.
- [22] Data Protection Working Party, *Opinion 05/2012 on Cloud Computing*. 2012, European Commission.
- [23] Pearson, S. and A. Benameur, *Privacy, Security and Trust Issues Arising from Cloud Computing*, in *IEEE CloudCom, 2010*. 2010. p. 693-702.
- [24] Google, *Security Whitepaper: Google Apps Messaging and Collaboration Products*. 2011.
- [25] Moyle, E., *Cloud computing vendor lock-in: Avoiding security pitfalls*. 2012.
- [26] Kesler, J.C., *Contractual and regulatory compliance challenges in grid computing environments*, in *Services Computing, 2005 IEEE International Conference on*. 2005, IEEE. p. 61-68.
- [27] Buecker, A., K. Lodewijkx, H. Moss, K. Skapinetz, and M. Waidner, *Cloud Security Guidance IBM Recommendations for the Implementation of Cloud Security*. 2009, IBM.
- [28] Jansen, W. and T. Grance, *Guidelines on Security and Privacy in Public Cloud Computing*. 2011, National Institute of Standards and Technology.
- [29] Federal CIO Council, *Guidelines for Secure Use of Cloud Computing by Federal Departments and Agencies - Draft Version 0.10*.
- [30] Hay, B., K. Nance, and M. Bishop, *Storm Clouds Rising: Security Challenges for IaaS Cloud Computing*, in *System Sciences (HICSS), 2011 44th Hawaii International Conference on*. 2011. p. 1-7.
- [31] Ibrahim, A.S., J.H. Hamlyn-Harris, and J. Grundy, *Emerging Security Challenges of Cloud Virtual Infrastructure*, in *APSEC 2010 Cloud Workshop*. 2010: Sydney, Australia.
- [32] Ristenpart, T., E. Tromer, H. Shacham, and S. Savage, *Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds*, in *Proceedings of the 16th ACM conference on Computer and communications security*. 2009, ACM: Chicago, Illinois, USA. p. 199-212.
- [33] Wei, J., X. Zhang, G. Ammons, V. Bala, and P. Ning, *Managing security of virtual machine images in a cloud environment*, in *2009 ACM workshop on Cloud computing security*. 2009, ACM. p. 91-96.

- [34] Pearson, S., *Taking account of privacy when designing cloud computing services*, in *Software Engineering Challenges of Cloud Computing, 2009. CLOUD '09. ICSE Workshop on*. 2009. p. 44-52.
- [35] Paquette, S., P.T. Jaeger, and S.C. Wilson, *Identifying the security risks associated with governmental use of cloud computing*. *Government Information Quarterly*, 2010. **27**(3): p. 245-253.
- [36] Ruan, K., J. Carthy, T. Kechadi, and M. Crosbie, *Cloud Forensics*. *Advances in Digital Forensics VII*, 2011: p. 35-46.
- [37] Taylor, M., J. Haggerty, D. Gresty, and R. Hegarty, *Digital Evidence in Cloud Computing Systems*. *Computer Law & Security Review*, 2010. **26**(3): p. 304-308.
- [38] Hay, B., K. Nance, M. Bishop, and L. McDaniel, *Are Your Papers in Order? Developing and Enforcing Multi-tenancy and Migration Policies in the Cloud*, in *System Science (HICSS), 2012 45th Hawaii International Conference on*. 2012. p. 5473-5479.
- [39] Heiser, J. and M. Nicolett, *Assessing the Security Risks of Cloud Computing*. 2008, Gartner.
- [40] Armbrust, M., A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, *A view of cloud computing*. *Communications of the ACM*, 2010. **53**(4): p. 50-58.
- [41] Zissis, D. and D. Lekkas, *Addressing cloud computing security issues*. *Future Generation Computer Systems*, 2012. **28**(3): p. 583-592.
- [42] Grobauer, B. and T. Schreck, *Towards incident handling in the cloud: challenges and approaches*, in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*. 2010, ACM: Chicago, Illinois, USA. p. 77-86.
- [43] Marston, S., Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, *Cloud computing — The business perspective*. *Decision Support Systems*, 2011. **51**(1): p. 176-189.
- [44] Szefer, J. and R.B. Lee, *A Case for Hardware Protection of Guest VMs from Compromised Hypervisors in Cloud Computing*, in *Distributed Computing Systems Workshops (ICDCSW), 2011 31st International Conference on*. 2011, IEEE. p. 248-252.
- [45] Oates, B.J., *Researching Information Systems And Computing*. 2006: Sage Publications.
- [46] Glisson, W.B., *The Web Engineering Security (WES) methodology*, in *School of Computing Science*. 2008, University of Glasgow: Glasgow.
- [47] Bulgurcu, B., H. Cavusoglu, and I. Benbasat, *Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness*. *MIS Quarterly*, 2010. **34**(3): p. 523-548.
- [48] Peltier, T.R., *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. 2001: Auerbach Publications.
- [49] Amazon Web Services, *Overview of Security Processes* 2011.
- [50] Glisson, W.B., L.M. Glisson, and R. Welland, *Secure Web Application Development and Global Regulation*, in *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*. 2007. p. 681-688.
- [51] European Parliament, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. 1995.
- [52] Vacca, J.R., *Computer forensics: Computer Crime Scene Investigation, 2nd Edition*. 2005, Hingham, MA: Charles River Media.
- [53] Grispos, G., W.B. Glisson, and T. Storer, *Using Smartphones as a Proxy for Forensic Evidence Contained in Cloud Storage Services*, in *System Sciences (HICSS), 2013 46th Hawaii International Conference on*. 2013, IEEE: Maui, Hawaii. p. 4910-4919.
- [54] PCI Security Standards Council, *Information Supplement: PCI DSS Virtualization Guidelines*. 2011.