**In what ways and to what extent do public-level cloud computing networks possess inherent security risks?**

Computer Science

May 2014

001480011

3766 Words

# Abstract

In a society which is becoming increasingly more dependent on technology, and likewise on cloud computing applications, it is essential to have an understanding of the security risks associated with this new-age technological dependency. This study seeks to answer the question: “in what ways and to what extent do public level cloud computing networks possess inherent security risks?” The study examines key attributes in the SaaS (Software-as-a-Service) cloud computing model, both as individual components and holistically, that introduce security risks into the cloud. These components include network security, data locality, data integrity, web application security, data breaches and segregation, vulnerability in virtualization, backup and disaster recovery, and identity management. Statistical analysis of numerous reports, surveys, and additional documentation will uncover evidence suggesting the presence of inherent security hazards in many SaaS cloud attributes as well as hazards that while non-inherent, still pose credible security risks. Security suggestions will be offered to mitigate some of these security risks. The evidence will further suggest that security risks with sufficiently large severity and scope can be generally associated with risks deemed to be inherent of SaaS in the cloud. The study concludes that public-level cloud computing networks do in fact possess a limited selection of inherent security risks.

(205 Words)

Table of Contents

[1. Abstract 2](#_Toc379904958)

[2. Introduction to Cloud Computing 4](#_Toc379904959)

[2.1 Cloud Service Models 4](#_Toc379904960)

[2.2 Cloud Deployment Models 5](#_Toc379904961)

[2.3 Justification for Investigation 6](#_Toc379904962)

[3. Security Issues in the SaaS Model 6](#_Toc379904963)

[3.1 Network Security 6](#_Toc379904964)

[3.2 Data Locality 7](#_Toc379904965)

[3.4 Web Application Security 8](#_Toc379904966)

[4.5 Data Breaches & Segregation 9](#_Toc379904967)

[3.6 Vulnerability in Virtualization 9](#_Toc379904968)

[3.7 Backup & Disaster Recovery 10](#_Toc379904969)

[3.8 Identity Management / Login Process 11](#_Toc379904970)

[4. Conclusion 12](#_Toc379904971)

[5. References 14](#_Toc379904972)

# Introduction to Cloud Computing

For years, network administrators and other technical professionals have illustrated the Internet and its underlying protocols simplistically as a cloud (). This image allowed developers to temporarily disregard the complex nature of cloud communication in favor of a visually oriented understanding that information would successfully flow from one Internet-connected network to another [1]. The cloud computing model in its most basic respect is defined by Merriam-Webster as “the practice of storing regularly used computer data on multiple servers that can be accessed through the Internet” [2].

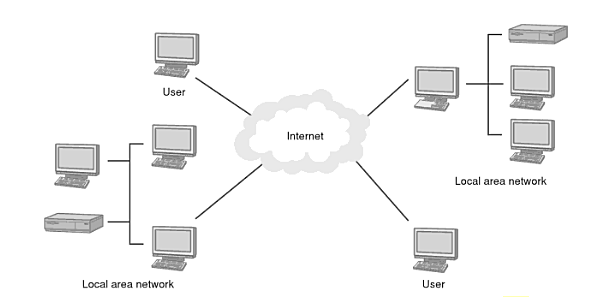


Figure 1 [1]

2.1 Cloud Service Models

In the past decade, the cloud computing model has been largely transformed from a conceptual computing idea, to a widely used concept that has become integral to the computing needs of a variety of users. With the model servicing a very large number of users, it is necessary to further define the parameters of cloud computing through the categorization of computing demands. The commonly agreed upon framework going by the acronym “SPI” is used to describe cloud computing services [3]. Table 1 outlines the components of the SPI framework.

|  |  |
| --- | --- |
| **Cloud Service Model** | **Characteristics** |
| Software as a Service (SaaS) | A complete software application with a user interface. |
| Platform as a Service (PaaS) | A platform within which developers can deploy their applications. A PaaS solution includes hardware (servers and disks), operating systems, development tools, and administrative tools. |
| Infrastructure as a Service (IaaS) | Provides machines, storage and network resources that developers can manage by installing their own operating system, applications, and support resources. |

Table 1 [1]

(263)

2.2 Cloud Deployment Models

The four primary cloud deployment models (private cloud, public cloud, community cloud, and hybrid cloud) may be either internally or externally implemented and specify how resources are shared within the cloud [1]. Table 2 illustrates each of the universally recognized cloud deployment models in terms of their defining characteristics:

|  |  |
| --- | --- |
| Deployment Model | Characteristics |
| Private Cloud | Owned by a specific entity and normally used only by that entity or one of its customers. The underlying technology may reside on – or off – site. A private cloud offers increased security at a greater cost. |
| Public Cloud | Available for use by the general public. May be owned by a large organization or company offering cloud services. Because of its openness, the cloud may be less secure. A public cloud is usually the least expensive solution. |
| Community Cloud | The cloud is shared by two or more organizations, typically with shared concerns (such as schools within a university). |
| Hybrid Cloud | A cloud that consists of two or more private, public, or community clouds. |

Table 2 [1]

2.3 Justification for Investigation

In today’s age of technology, one can very easily see the increasing demand for variations of the SaaS model through popular everyday applications such as Facebook, Twitter, YouTube, Dropbox etc. Social networking and file sharing websites are beginning to take an increasingly more significant role in society as businesses, government services, educational institutions and other essential societal aspects integrate features of the cloud. It is essential that a basic understanding of the risks associated with cloud integration be developed in order to protect services we depend on everyday. The following investigation seeks to answer the question: *“In what ways and to what extent do public-level cloud computing networks possess inherent security risks?”*

# Security Issues in the SaaS Model

In the Software as a Service (SaaS) model, the client has to trust that the service provider has proper security measures put in place. This “hands off” approach makes it difficult for the user to ensure that the right security measures are in place and that applications will be available when in demand [4]. “In a recent survey of 4,500 high-level IT professionals in 83 countries, the Information Systems Audit and Control Association (ISACA) found that security risk is the most widely cited inhibitor to Software-as-a-Service (SaaS) adoption [5].“ The level to which an SaaS model can be deemed secure can be determined through the examination of several key areas for potential malicious exploitation and inherent downfalls. This section aims to examine the most significant of these areas.

3.1 Network Security

Whether a software application based upon the SaaS deployment model is utilized for private or corporate purposes, it is essential that its clients be guaranteed complete confidentiality in the transportation of their data. The task of transferring data back and forth from a client’s computer terminal to a remote SaaS vendor location while maintaining its integrity has become more and more fraught with unique challenges. As supporting infrastructure for internet servers increases, the number of potential points in which one’s data may be intercepted increases also. “…malicious users can exploit weaknesses in network security configuration to sniff network packets [4].”All data transmitted over network infrastructure must be secured in order to prevent leakage of client information [4].

In an effort to combat the interception of a client’s valuable information, the use of data encryption algorithms can be an invaluable tool for SaaS vendors. The current standards of cryptology protocols TLS 1.0 and SSL 3.0 both prevent eavesdropping of data by ensuring data cannot be read without the encryption key [6]. However, the improper implementation of cryptologic protocols or failure to implement cryptologic protocols can facilitate relatively easy access to clients’ data by malicious parties.

Recent studies published by The Open Web Application Security Project (OWASP) state that “[SaaS] applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic [7].” And that “when crypto is employed, weak key generation and management, and weak algorithm usage is common… [8]”. This suggests that although methods of ensuring secure data transportation are available, not all SaaS vendors choose to implement it or are able to implement it with a high degree of effectiveness. This has the potential to pose many serious security risks; however, given that preventative measures are available to combat these risks, the SaaS model in itself does not pose inherent network security risks to its clientele. Instead, some vendors may be considered negligent for failing to implement some network security measures correctly.

Security Suggestion:

To combat lapses in Software-as-a-service network security, it is recommended that some method of data encryption protocol be used when transferring data over the network. In order to prevent SaaS vendors from failing to implement effective measures to encrypt user data, it is suggested that the vendors be legislated to do so. SaaS vendors additionally should be subjected to random inspections of network security protocols under this new legislation. This would ensure that the vast majority of vendors correctly implement current security protocols and prevent the malicious exploitation of data on cloud computing networks as encryption measures render it practically useless.

3.2 Data Locality

When using the SaaS computing model, customers using the application often store personal or corporate data on SaaS storage media. In this model, customers often do not know precisely where in the world their data is getting stored [4]. This while seemingly insignificant, identifies a sizable security concern with respect to country-specific privacy legislation. In many countries, “…certain types of data cannot leave the country because of potentially sensitive information” [4]. Depending on the technicalities of each country’s legislative movements, an SaaS vendor may be encouraged to outsource storage of client data or to remain in-country. SaaS vendors possessing over-the-border infrastructure sacrifice client convenience for loss of complete control over data security.

In October of 1998, the European Commission’s Directive on Data Protection went into effect prohibiting the transfer of personal data to countries not in the European Union (EU) or that do not meet the EU’s adequacy standard of privacy protection [9]. This approach to data protection proved to be very different from rules existing in countries like the United States who adopted a sectoral approach relying on a mix of legislation, regulation and self-regulation [9]. The multiple different approaches to data security legislation taken by countries creates a tangled web of legal guidelines. Conflicting interpretations of data privacy measures create ambiguity in the utilization of any one legislative document and in turn creates the potential for the disclosure of client data by terms in which the client is unfamiliar. This not only constitutes a security risk, but one that clients have no control over and which SaaS vendors also have little influence over. As a result, when client data is stored across borders, an inherent security risk is introduced via worldwide legislative interaction.

Security Suggestion:

In order to mitigate this ambiguity, international legislation should be established to specifically outline a code of conduct when dealing with the transfer and storage of information across international borders. The “terms of service” for SaaS applications should be updated to include international legislation and should include verification methods (i.e. checkboxes) to ensure users read and understand what legal rulings their information is subject to. These changes if implemented universally, could greatly reduce and / or eliminate ambiguity in differing privacy legislations and remove data locality as a security risk to the SaaS cloud computing model.

3.4 Web Application Security

One of the requirements for an SaaS application is that it has to be used and managed through the internet with the use of an internet browser [4]. “Since the web applications and SaaS are tightly coupled in providing services to the cloud users, most of the security threats of web applications are also posed by the SaaS model in the cloud [4].” It is therefore essential that SaaS vendors not only employ the use of network security protocols, but also implement security measures at the application level [4]. Application level security measures when implemented correctly and paired with security on the cloud network enables SaaS administrators to ensure that client data is guarded against attack.

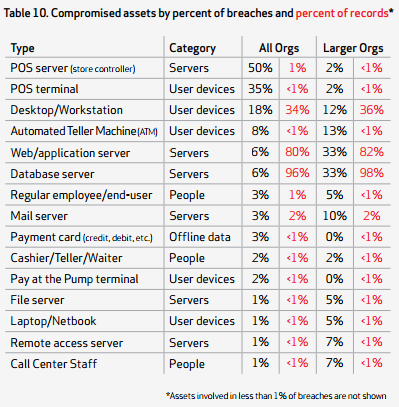


Figure [15]

A 2012 study conducted by Verizon’s RISK Team in association with numerous acclaimed institutions noted that 6% of breaches compromising assets were directed at web applications (Figure 2). The same study conducted a year later (in 2013), showed that 10% of breaches compromising assets were vectored at web applications. This 4% increase in application level attacks over just a one year period represents a significant change in the focuses of hackers today. Whether this is due to insufficient preventative measures or a more formidable and technologically educated opponent remains unclear however, it illustrates the need for continued advancements in web application security to deter hackers from targeting web applications. Ambiguity in the reasons behind compromised web applications does not conclusively point out web application security as possessing inherent security flaws, however without a focused effort on preventing attacks at this level, it remains logical to project that the number of specific targeted attacks on web applications will continue to rise. Although at this time, web applications do not constitute inherent risks, this potential rise in attacks targeting web applications may lead to new evidence for becoming one.

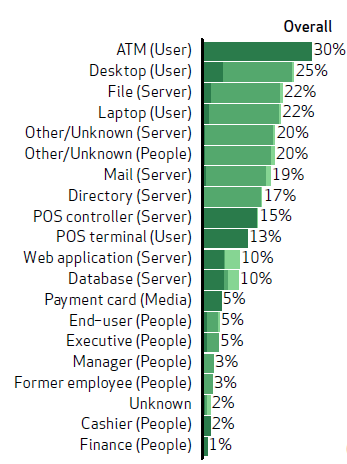


Figure [13]

4.5 Data Breaches & Segregation

Data breaches, or incidents in which confidential information has potentially been viewed or used by an individual unauthorized to do so [10], continue to spark debates over the security of the SaaS model as the model becomes increasingly more popular. Research has shown that “Since data from various users and business organizations lie together in a cloud environment, breaching into the cloud environment will potentially attack the data of all the users. Thus the cloud becomes a high value target.” [4] The storage of large quantities of data in the same location while being linked by a single SaaS user interface, the same type of interface promising widespread accessibility to clients, proves to be a detriment to security as a single incident may expose the information stored by many clients. Of course, SaaS administration does have the option to intelligently segregate user data and ensure that a mass data breach does not in fact occur, however the concept that one client’s data is stored alongside multiple other clients’ information creates an inherent vulnerability for the lot.

“A recent study by the Ponemon Institute revealed that 65 percent of respondents who shared consumer data with third-party vendors had experienced a breach involving stolen or lost information, and 64 percent reported more than one of these incidences [8].” Statistics such as these imply not only that data breaches are relatively common place in the SaaS model, but reinforce the vulnerability of data stored in this manner. It also implies that despite knowledge of this issue, security measures intertwined in the SaaS system fail to adequately deal with such incidents. One explanation for this may be the involvement of vendor employees in data breach incidents. With the security of SaaS consumer interfaces in the spotlight, security checks for employees of vendors may be inadequate, resulting in the continuation of data breach incidents. However, regardless of the reason for its relatively frequent occurrence, the fact remains. The SaaS model is inherently vulnerable to data breaches for the shear bulk of information accessible through one system.

3.6 Vulnerability in Virtualization

The creation of virtual replications of computer architecture such as the CPU, storage, database, memory etc. remains an essential backbone to the Software-as-a-Service cloud computing model. Virtualization technologies enable cloud business models to support multitenancy and shared resource platforms [3]. Through the virtualization of personal computing components for use on the cloud, many security risks are introduced that are compounded by the critical role of virtualization in cloud infrastructure. For example, “ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization which is not met completely in today’s scenario [as] many bugs have been found in all popular VMMs (Virtual Machine Managers)... [4]”

A 2009 report on virtualization vulnerabilities and threats cited the following as known exploits of VMMs: VM Sprawl, Hyperjacking, VM Escape, Incorrect VM Isolation, Denial of Service, VM Poaching / Resource Hogging, Unsecured VM Migration / VMotion, and Host & Guest Network Communication Vulnerabilities [11]. These eight exploits attack a fundamental part of cloud computing and in doing so, open up additional components of the computing model to attack. As such, security measures must be enacted specific to individual vulnerabilities in virtualization in order to prevent security risks in all aspects of the computing model. As a core element of SaaS in the cloud, it can be reasoned that virtualized components should be one of the most secure points in the cloud, however evidence suggests that this may not be the case. A survey on cloud computing established that, “a perfection of [security] properties… is yet to be completely achieved in VMMs [4].” It can be concluded from this that due to the instrumental roll virtualization plays in cloud security and the presence of unsolved VM exploits, vulnerabilities in virtualization do indeed pose an inherent security risk.

Security Suggestion:

In order for vulnerabilities in virtualization to be eradicated from the cloud computing model, it is first and foremost essential that the exact methods of exploitation be known to SaaS vendors and is therefore recommended that companies specializing in penetration testing be hired. These companies would provide specific feedback as to what makes each virtualization exploit possible and allow SaaS vendors to deal with these threats more efficiently and effectively.

3.7 Backup & Disaster Recovery

As SaaS applications make storing personal and corporate information increasingly more convenient, the need to ensure that stored client data remains readily available is growing accordingly. Users of SaaS applications are able to rely with increasing exclusivity on these applications and in doing so, trust that their data is accessible at all times. For this reason, “the SaaS vendor needs to ensure that all sensitive…data is regularly backed up to facilitate quick recovery in case of disasters [4].” SaaS vendors should create a DRP (Disaster Recovery Plan) that effectively minimizes risk to users from delays in service in the event that disruptive events occur [12]. A classification like that shown in Figure 4 can be used to rank the time which an SaaS vendor deems to be acceptable to the client [12]. Given the potential for a significant difference in resources devoted to backup and disaster recovery plans, the level to which an SaaS vendor can be deemed unsecure is variable.

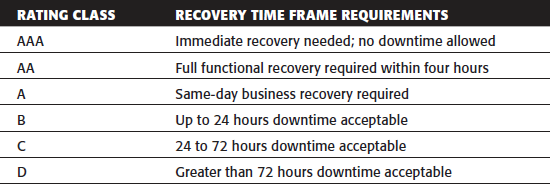


Figure [12]

When further examining the secure backup and recovery of client information in case of a disaster, its security is not only vulnerable in that data can be lost / inaccessible but also in the level to which it resists attacks while in storage. On many SaaS applications, data is not encrypted by default and it is left up to users to encrypt their data and backups to prevent access and tampering by unauthorized parties [4]. Leaving this responsibility up to the SaaS client adds significant risk to maintaining security as vendor policies have no power to regulate a client’s encryption. While this does give the client the burden of responsibility for lost data, it also puts the SaaS vendor’s infrastructure and other client data at risk as a target for unauthorized intrusion. Due to the highly individualized nature of SaaS vendors regarding backup and disaster recovery policies, it can be concluded that an inherent security risk present in all systems is not created however; individual security risks may be present in a particular SaaS vendor’s model.

3.8 Identity Management / Login Process

SaaS applications are designed to allow clients to access software, settings and related data from any terminal with a connection to the internet. In order to provide this capability, SaaS platforms must be able to identify valid users of the system and manage the level to which individual users have access to different parts of the system. SaaS vendors have adopted the use of Usernames and Passwords or Passphrases as a means for identifying valid users of the system, while denying access to invalid users.

“User authentication is performed by checking the username and password values from the login and evaluating them to ensure they are valid entries in the system [6].” However, Username and Password authentication can only be as secure as the user-chosen login criteria. A 2013 report published by Verizon cited that 76% of network intrusions exploited weak or stolen credentials [13]. It is therefore essential that SaaS vendors enforce minimum password requirements that prompt users to create alphanumeric passwords containing a preselected minimum number of characters. Administrative requirements like these provide added security as passwords become more complex and therefore less likely to be cracked. Though the odds of an unwanted user accessing an SaaS system employing password security measures are quite often negligible, security of client data stored in password protected systems cannot be completely guaranteed.

In order to minimize attempts to exploit this security issue in systems employing password protection, SaaS vendors may choose to employ other administrative measures such as the use of account lockouts [6]. When implemented correctly, account lockouts prevent unauthorized parties from attempting too many incorrect passwords and close off opportunities to exploit the password system. Though additional security measures like this have become readily available to SaaS vendors and have the potential to significantly reduce security loopholes in identity management, it does not eliminate all such exploits. As the technologies and algorithms behind today’s login processes continue to develop, the knowledge and resources of parties who aim to counter these processes do likewise. It can therefore be deduced that the favored security measures of today’s identity management systems do in fact represent a small, but ever-present inherent security risk in the SaaS model.

Security Suggestion:

In order to mitigate problems seen through password / passphrase based user authentication, it is suggested that SaaS vendors implement alternate methods of authentication, for example: facial recognition, voice recognition, biometric authentication etc. These methods when added to password / passphrase authentication or used alone would limit the extent to which passwords could be guessed, stolen, or otherwise bypassed and help close the security loopholes in identity management.

# Conclusion

As today’s society shifts towards an embrace of continual technological advancement, public-level cloud computing networks are becoming increasingly more popular for both private and corporate purposes. As demands on the SaaS cloud computing model continue to grow, new hardware and software infrastructure must grow accordingly to support the new demand. The continual modularized addition of resources aimed at improving the SaaS model creates unique security challenges. These challenges manifest between developing layers of essential cloud elements including Network Security, Data Locality, Data Integrity, Web Application Security, Data Segregation, Virtualization, Backup and Disaster Recovery and Identity Management.

|  |  |
| --- | --- |
| **Security Risk** | **Conclusion** |
| Network Security | No Inherent Risk. Some vendors may be negligent. |
| Data Locality | Inherent Risk. Introduced through worldwide legislative interaction. |
| Web Application Security | No Inherent Risk. Rising rate of attacks may lead to becoming one. |
| Data Breaches and Segregation | Inherent Risk. Shear bulk of information accessible at once. |
| Vulnerability in Virtualization | Inherent Risk. Instrumental role in cloud security / unsolved VM exploits. |
| Backup and Disaster Recovery | No Inherent Risk. Potential for individualized risk in particular SaaS vendors. |
| Identity Management / Login Process | Inherent Risk. Small but ever-present. |

It is evident that although each of these elements possess a capacity within themselves to introduce security risks into the SaaS cloud environment, each differs in the extent to which potential risks are likely and to which risks are created inherently as a result of the SaaS cloud environment.

Table 3

Through this study, it was revealed that four out of seven cloud elements examined pose an inherent security risk to cloud infrastructure (See table 3). While the majority of elements examined do show evidence of inherent security risks, there is neither sufficient evidence alone pointing to an inherently vulnerable SaaS cloud model nor sufficient grounds to declare this model free from inherent risk. However, further in-depth examination of elements of the cloud deemed to be inherently at risk reveals that the severity and scope of these risks is generally quite large.

Given that the elements examined in this study do not account for all potential security risks present in a continually developing SaaS model, and that solutions to existing security risks will be engineered while new security challenges are introduced, it is reasonable to assume that the number of inherent, severe and far-reaching risks will balance with those that are not inherent and of lesser severity proportional to the results established in this study. As such, this study concludes that public-level cloud computing networks do in fact possess a limited selection of inherent security risks. Given this result, future investigations may examine in depth, the implications of these security risks and may attempt to develop new solutions.

# References

|  |  |
| --- | --- |
| [1] | K. Jamsa, "Cloud Computing, Burlington", MA: Jones & Bartlett Learning, 2013. |
| [2] | Merriam-Webster. (2013). *Cloud Computing* [Online]. Available: http://www.merriam-webster.com/dictionary/cloud%20computing. [Accessed 24 June 2013]. |
| [3] | T. Mather, S. Kumaraswamy and S. Latif, "Cloud Security and Privacy", Sebastopol, CA: O'Reilly Media, 2009. |
| [4] | S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications,* vol. 34, no. 1, pp. 3-8, 2010. |
| [5] | J. Manciocchi. (2013, April 10). *10 Tips to Ensure Data Security in the Cloud* [Online]. Available: http://saasmarkets.com/10-tips-to-ensure-data-security-in-the-cloud/. [Accessed 07 September 2013]. |
| [6] | Web and Flow. (2013). *Security and SaaS* [Online]. Available: http://webandflo.com/docs/waf\_paper\_saas\_security.pdf. [Accessed 12 August 2013]. |
| [7] | The OWASP Foundation. (2010)*. OWASP Top Ten Project* [Online]. Available: https://www.owasp.org/index.php/Category:OWASP\_Top\_Ten\_Project#tab=OWASP\_Top\_10\_for\_2010. [Accessed 12 August 2013]. |
| [8] | The OWASP Foundation. (2013). *OWASP Top Ten Project* [Online]. Available: https://www.owasp.org/index.php/Category:OWASP\_Top\_Ten\_Project#tab=OWASP\_Top\_10\_for\_2013. [Accessed 12 August 2013]. |
| [9] | export.gov. (2013, January 7). *U.S. - EU Safe Harbor Overview* [Online]. Available: http://export.gov/safeharbor/eu/eg\_main\_018476.asp. [Accessed 25 September 2013]. |
| [10] | R. L. Krutz and R. D. Vines, "Cloud Security", Indianapolis: Wiley Publishing, 2010. |
| [11] | M. Rouse. (2010, May). *Data Breach* [Online]. Available: http://searchsecurity.techtarget.com/definition/data-breach. [Accessed 07 September 2013]. |
| [12] | V. Vaidya, "Virtualization Vulnerabilities and Threats: A Solution White Paper," RedCannon Security, 2009. |
| [13] | Verizon RISK Team, "2013 Data Breach Investigations Report," Verizon, 2013. |
| [14] | ProofPoint. (2013, February 27). *Rising Data Breaches Demand SaaS Security Solutions* [Online]. Available: http://www.proofpoint.com/about-us/security-compliance-and-cloud-news/articles/rising-data-breaches-demand-saas-security-solutions-393659. [Accessed 07 September 2013]. |
| [15] | Verizon RISK Team, "2012 Data Breach Investigations Report," Verizon, 2012. |