Information Security and the Cloud

INFORMATION SECURITY AND THE CLOUD

BY

STEPHEN FLAAEN

A Thesis Submitted to The Honors College

In Partial Fulfillment of the Bachelor's degree
With Honors in

Management Information Systems

The University of Arizona

May 2012

Approved by:

Dr. Alexandra Durcikova
Department of Management Information Systems

STATEMENT BY AUTHOR

SIGNED: ____________________

The University of Arizona Electronic Theses and Dissertations Reproduction and Distribution Rights Form

Name (Last, First, Middle) FLAAEN, STEPHEN THOMAS

Degree title (eg BA, BS, BSE, BSB, BFA): BSBA

Honors area (eg Molecular and Cellular Biology, English, Studio Art): Management Information Systems

Date thesis submitted to Honors College: May 7, 2012

Title of Honors thesis: INFORMATION SECURITY AND THE CLOUD

:The University of Arizona Library Release	I hereby grant to the University of Arizona Library the nonexclusive worldwide right to reproduce and distribute my dissertation or thesis and abstract (herein, the "licensed materials"), in whole or in part, in any and all media of distribution and in any format in existence now or developed in the future. I represent and warrant to the University of Arizona that the licensed materials are my original work, that I am the sole owner of all rights in and to the licensed materials, and that none of the licensed materials infringe or violate the rights of others. I further represent that I have obtained all necessary rights to permit the University of Arizona Library to reproduce and distribute any nonpublic third party software necessary to access, display, run or print my dissertation or thesis. I acknowledge that University of Arizona Library may elect not to distribute my dissertation or thesis in digital format if, in its reasonable judgment, it believes all such rights have not been secured. Signed: Date: 5/7/12

Last updated: Nov 15, 2009

INFORMATION SECURITY AND THE CLOUD

BY

STEPHEN FLAAEN

A Thesis Submitted to The Honors College

In Partial Fulfillment of the Bachelor's degree
With Honors in

Management Information Systems

The University of Arizona

May 2012

Approved by:

____

Dr. Alexandra Durcikova
Department of Management Information Systems

STATEMENT BY AUTHOR

I hereby grant to the University of Arizona Library the nonexclusive worldwide right to reproduce and distribute my thesis and abstract (herein, the “licensed materials”), in whole or in part, in any and all media of distribution and in any format in existence now or developed in the future. I represent and warrant to the University of Arizona that the licensed materials are my original work, that I am the sole owner of all rights in and to the licensed materials, and that none of the licensed materials infringe or violate the rights of others. I further represent that I have obtained all necessary rights to permit the University of Arizona Library to reproduce and distribute any nonpublic third party software necessary to access, display, run, or print my thesis. I acknowledge that University of Arizona Library may elect not to distribute my thesis in digital format if, in its reasonable judgment, it believes all such rights have not been secured.

SIGNED: _____________________________

Table of Contents

Table of Figures 4

Table of Tables 5

I. Abstract 1

II. Introduction 2

III. Cloud Computing Providers 5

1. Google 5
2. Amazon 6
3. IBM 7
4. Oracle 7
5. Microsoft 8

IV. Laws Regarding Consumer Privacy 10

The Electronic Communications Privacy Act (1986) 10

HIPAA (1996) 10

Communications Decency Act (1996) 12

Payment Card Industry (PCI) Data Security Standard (DSS) 12

Various Laws Regarding Illegal Material and Copyright Infringement 14

V. Privacy 16

VI. Gaps in Security 18

VII. Conclusion 21

Bibliography 24

Appendix A – Hosted Service Provider PCI DSS Regulations 27

Appendix B – Cryptography 29

Table of Figures

Figure 1 – HIPAA Violation Penalties (American Medical Association) 11
Figure 2 – PCI Data Security Standards (PCI Security Standards Council LLC, 2010) 14

Table of Tables

Table 1 – Google Apps 5
Table 2 - Amazon Web Services 6
Table 3 - IBM.. 7
Table 4 - Oracle 8
Table 5 - Microsoft 9

I. Abstract

In today’s business environment companies are looking for ways to differentiate their services as well as maintain low costs to provide these services. Leveraging information technology has proved to be one of the most successful ways to accomplish this. One of the rapidly growing technologies that both small and large companies can utilize is cloud computing. A ubiquitous term for many IT managers and C-level executives, cloud computing is in fact a poorly understood term to many outside the realm of information technology. This paper develops a clear definition of cloud computing and also discusses information security in cloud computing. Information security has become a large concern for businesses because consumers are putting their trust into these companies’ hands and want to keep sensitive information, such as credit card numbers and medical records, protected. In addition, this paper introduces privacy laws that every company using cloud computing should be familiar with. Specifically, laws dealing with patient healthcare information and credit card safety are discussed in detail. I conclude with security guidelines for businesses that use CC services.

II. Introduction

Cloud computing is a phrase that is increasingly being used today in business as a way to stay on the cutting of edge of technology. According to estimates by Merrill Lynch in 2013 cloud computing is estimated to be a $160 billion industry, including "$95 billion in business and $65 billion in online advertising", which will account for 12 percent of total corporate computing (Valacich, George, & Hoffer, 2012). However, frequently cloud computing, henceforth referred to as CC, is not fully understood when used, and is used as a blanket term for all different matters of information technology. What does cloud computing mean? An informal definition can be created by explaining what "cloud" and "computing" mean. The cloud comes from the fact that it is "entirely virtual, invisible to the user, potentially located anywhere in the world and requires no client installations or special hardware," while the computing refers to the fact that this has to deal with computers (Parks & Harvey, 2008).

The purpose of this paper is to discuss the relationship between CC and information security. To do this the web of relationships between CC and information security must first be untangled, starting with listing the companies that provide CC services. This will be followed by a discussion and analysis of the laws concerning consumer privacy, with special emphasis put on the laws dealing with patient healthcare information and credit card safety. Next, an in depth discussion on privacy and its impacts on consumers will take place followed by a section on the gaps in security that have been discovered. Finally a conclusion will be presented and security guidelines will be given for businesses that use CC services.

Before any further progress is made in this paper, a much more formal, structured definition of CC is needed. CC is best defined as: a way for a business to contract with another firm, called a service-provider, that provides computing resources (such as networks, servers, storage, applications, and services) over the Internet in a convenient and flexible way that provides on-demand resources and thus requires minimal management effort or interactions with the service-provider (Amrhein & Quint, 2009) (Fitzgerald, Dennis, & Durcikova, 2011) (Mell & Grance, 2010) (Mullan, 2010). There are three types of cloud computing services: Public (handled by a third party vendor), Private (maintained by the company itself) and Hybrid (combination of public and private) (Amrhein & Quint, 2009).

The three types of CC are very important to distinguish from each other. The public cloud is the most prevalent type of CC and is the one which most are familiar with. The public cloud can be used by just about anyone, businesses (e.g., a business renting space from Amazon's AWS for their server), governments (using Gmail, Blackberry or Microsoft as their email provider), or regular people. The benefit of a public type of Cloud is that it is scalable, meaning that users only need to pay for what they use, providing substantial cost savings over the traditional method of purchasing and maintaining server clusters. A more thorough definition of a public cloud is "one that is made in a pay-as-you-go manner available to the general public. It is sold as utility computing." (Armbrust, et al., 2010). The private cloud is one instance of CC in which a business maintains and controls its own cloud network. This provides more security for the company in that it allows them to only allow certain users on the network. It allows the business to pool its own resources (e.g. having all departments use one network instead of each department having their own network). Private cloud refers to the internal data centers of a business or other organization, not made available to the general public (Armbrust, et al., 2010). A hybrid cloud is one in which both public and private instances of CC are used. This can be done because a company wants the cost savings of using a public cloud such as Amazon's AWS for the HR department, and maintaining a private cloud for the engineering department because of the trade secrets maintained in the department.

Two more very narrow applications of CC exist, namely Software as a Service (SaaS) and Infrastructure as a Service (IaaS). SaaS refers to a specific application or solution deployed in an on-demand way (Mullan, 2010). Whereas IaaS is more reliant upon providing hardware and administrative services that are needed to store applications and a platform to run the applications (Bhardwaj, Jain, & Jain, 2010). Both SaaS and IaaS are integral parts of CC, but a CC vendor does not necessarily need to provide both in order to be classified as such. A vendor such as Google with their product Google Apps provides both SaaS and IaaS. Using their popular email client, Gmail, as an example, the storage of email that Google provide is classified under IaaS, while the Gmail itself is SaaS.

III. Cloud Computing Providers

There are many different providers of many different CC services to businesses both large and small. It is important to note which of these CC companies provide SaaS and which provide IaaS. Some of the largest companies providing CC services are Google, Amazon, IBM, Oracle, and Microsoft (Amrhein & Quint, 2009). Out of these major providers, specific focus will be given to Google, Amazon, and IBM because of their size and that they provide both SaaS and IaaS.

1. Google

Google, through their Google Apps program, provides five distinct levels of CC services: Google Apps (free), Google Apps for Business, Google Apps for Government, Google Apps for Education, and Google Apps for Nonprofit (Google Apps for Business). The major differences in these services are the features available and the cost (see Table 1 – Google Apps). For Google Apps (free), there is no cost, but limited access to the suite of applications which Google provides; those who have Gmail accounts are using Google Apps (free) (Google Apps for Business). Although the level of services provided and cost are different between each level all of the Google Apps platforms work as both SaaS and IaaS.

Table 1 – Google Apps

Features	Cost
Google apps for business are: Calendar, Docs, CloudConnect, Groups, Sites, Video, Mobile Applications and their app marketplace which consists of web applications that integrate with Google.	Business, Government and Nonprofits with over 3,000 users: Annual plan of $50 per user account per year. Flexible plan of $5 per user account per month. Education and US 501(c) (3) accredited Nonprofits with less than 3,000 users: No charge.

2. Amazon

The next major provider to focus on is Amazon. Like Google, Amazon also has a suite of platforms, collectively called Amazon Web Services (AWS), that can be used and are considered SaaS, IaaS or a combination of the two (Amazon Web Services). AWS currently has 14 different applications and the large number platforms offered makes Amazon one of the leading CC providers in terms of variety (Amazon Web Services). Of the 14 different platforms they offer the two most well-known are Amazon Elastic Compute Cloud (also known as EC2) and Amazon Simple Storage Service (also known as S3) (Amazon Web Services). Both EC2 and S3 are considered IaaS because Amazon is providing the infrastructure, in the case of EC2 servers and S3 storage space, while Amazon Relational Database Service (RDS) is considered both IaaS and SaaS because they provide the software to configure the database and the space to store the database (Amazon Web Services). Features and cost of these services provided by Amazon are described in - Amazon Web Services 2.

Table 2 - Amazon Web Services

Features	Cost
Scalability, the ability for a user to add or subtract the amount of the platform used whenever needed, is the biggest selling point of AWS. The variety of services offered and compatibility with Linux/UNIX and Windows, the most commonly used business operating systems, are also features that make Amazon and AWS attractive as a CC provider.	• EC2 ranges from \$0.085 to \$2.10 per hour run on a Linux/UNIX system and from \$0.12 to \$2.60 per hour run on a Windows system. • S3 ranges from \$0.125 per GB[1] under 1 TB[2] per month down to \$0.055 per GB for any amount over 5000 TB. There are also costs for transferring data out of their system back to the clients, which are entirely dependent upon the amount of data transferred.

[1] GB stands for gigabyte, which is 10^9 bytes. Approximately 330 three minute songs can be considered 1 GB.

[2] TB stands for terabyte, which is 10^{12} bytes. Approximately 130,000 three minute songs can be considered 1 TB.

3. IBM

Like Amazon, IBM has a suite of offerings that is grouped together and called IBM SmartCloud. SmartCloud offers both IaaS and SaaS. Under IaaS they have SmartCloud Enterprise, which is their storage solution, and Smart Business Desktop, which allows a user to create a virtual desktop on IBM's system. IBM also offers SmartCloud Archive, Managed backup services, and Virtualized Server Recovery for automated information backed-up, which are a mixture of both SaaS and IaaS (IBM Corporation). IBM also classifies their Hosted Application Security Management, Hosted Mobile Security Management and Managed Security Services Management programs as IaaS, however, because of the definitions established previously, for this paper these services are classified as a mix of SaaS and IaaS. For their SaaS offerings, IBM has many features, such as Blueworks Live, that build upon what they have done for years, IT consulting and business process management, and uses the internet, through CC, to continue to offer these services virtually (see Table 3 - IBM for details).

Table 3 - IBM

Features	Cost
IBM has a variety of services they offer similar in number to Amazon. However, IBM's services are more suited towards transitioning their traditional business and technology consulting to the internet.	The prices vary depending on what service is selected. Services that store information are charged on a per GB usage rate with additional fees for extra programs. For services that do not use mass storage, they are charged on a per user per month basis.

4. Oracle

Oracle has SaaS, which they call Oracle on Demand and works with other companies to provide IaaS. As part of their SaaS Oracle has two options that users can choose from: hosted and managed applications and SaaS applications; currently only Oracle CRM On Demand is available in the SaaS application category (Cloud Computing | Oracle). Oracle is unique among the CC providers in that they do not directly offer IaaS. However, because of the variety of proprietary software and hardware that Oracle owns, they play a major part in most of the servers that actually hold the data. For example Oracle works with Amazon to allow companies to deploy Oracle software (usually server virtualization) on Amazon machines. Oracle also offers a public cloud available to service owners, developers and end users. On this public cloud Oracle offers both IaaS and SaaS in the form of Fusion Customer Relationship Management, a software that allows a business to track multiple facets of sales, Fusion Human Capital Management, a software that lets a business manage its employees more efficiently, a social network that allows secure, online collaboration between users, a location for creating and storing code written in Java, and a location for developing, testing and implementing databases. An explanation for the lack of pricing information is found in Table 4 - Oracle.

Table 4 - Oracle

Features	Cost
Hosted and managed applications, Oracle CRM On Demand as a stand-alone application. They also provide vital software and hardware to other CC providers.	Prices are based on quotes; however, Oracle does have separate fee schemes, one for pay-per-use and another for a fixed licensing fee.

5. Microsoft

Microsoft offers many different instances of both SaaS and IaaS. Two of the most well-known are the Microsoft Azure platform and the Microsoft Office 365 (Cloud Computing | Productivity Tools | Cloud Hosting | Microsoft Cloud). Azure is the typical IaaS allowing the user to deploy their own applications on hardware owned by Microsoft. Microsoft also offers other common services an IaaS, such as mass storage, virtual machines and compatibility with a database (Microsoft Corporation). Microsoft Office 365 is very similar to the SaaS products offered by both IBM and Google. Both offerings emphasize collaboration from anywhere and ease of use available in a full productivity suite that can be used online (Microsoft Corporation). Although the services are similar to those of Google and IBM, the pricing structures of each are different and can be found in Table 5 - Microsoft.

Table 5 - Microsoft

Features	Cost
Provides a productivity suite that is very similar to that of Google and IBM. Emphasize all of their services are backed-up by the reliability of Microsoft, even offer finically backed uptime guarantee. (Microsoft Corporation)	The cost for Azure runs from $0.04 per computer hour to $0.96 per computer hour. The cost for Office 365 runs from $6 per month per user to $10 per month per user

IV. Laws Regarding Consumer Privacy

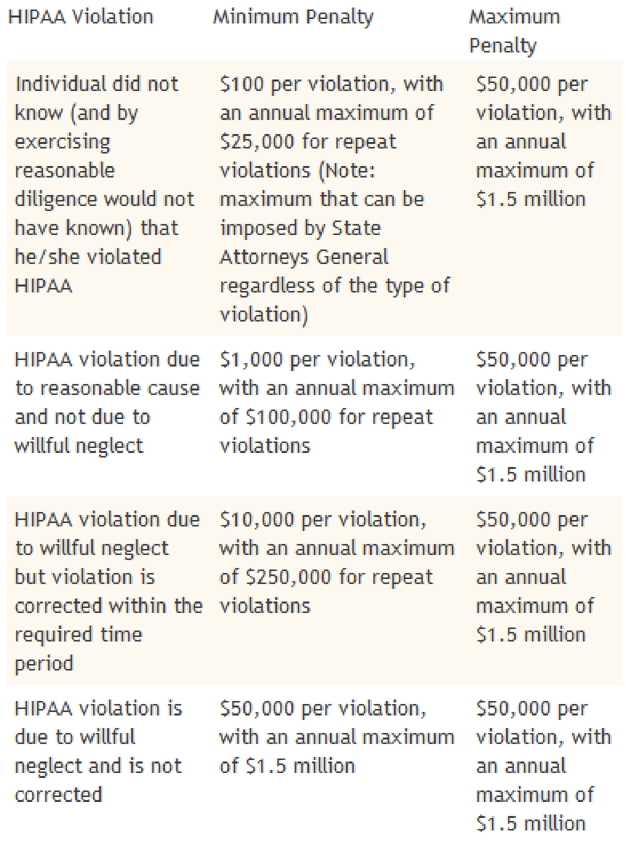
There are several laws that protect consumer privacy in the area of electronic data communication. Each of these laws is discussed next.

The Electronic Communications Privacy Act (1986)

The Electronic Communications Privacy Act of 1986 (ECPA) was passed to extend "restrictions on wiretaps beyond telephone calls to apply to electronic data transmissions" (Department of Homeland Security/Office for Civil Rights and Civil Liberties). The ECPA was the first piece of legislation to deal with modern information security issues in the personal computer era. The ECPA "protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers"; this was the first law to deal with the protection of electronic data in transit and data at rest (Department of Homeland Security/Office for Civil Rights and Civil Liberties). With the passage of the ECPA, violating electronic data protection became a felony and those "who illegally intercept communications face: criminal penalties of up to 5 years in jail or civil damages up to $10,000 per violation" (Legal Information Institute). The ECPA was a crucial step on the path of information privacy and paved the way for the privacy laws that followed it.

HIPAA (1996)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) gives the consumer right over their health information and "sets rules and limits on who can look at and receive your health information" (US Department of Health & Human Services). HIPAA also sets who is legally required to follow its laws, health plans, health care providers and health care clearinghouses are all required to abide by HIPAA regulations. Interestingly, organizations like life insurers, employers, workers compensation carriers, some schools and school districts, some state agencies, some law enforcement agencies and many municipal offices are not required to abide by HIPAA (US Department of Health & Human Services).



HIPAA Violation	Minimum Penalty	Maximum Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

Figure 1 – HIPAA Violation Penalties (American Medical Association)

The repercussions from violating portions of HIPAA are very strict and taken very seriously in the medical community. The American Medical Association has a system of fines they levy against violators, shown in Figure 1 – HIPAA Violation Penalties. In fact, in 2010 a doctor, for the first time, was sentenced to time in prison for illegally accessing confidential medical records (Dimick, 2010). The doctor in this case managed to access the confidential records of his superiors as well as celebrity clients of the hospital in which he worked; all said he illegally accessed medical records 323 times (Dimick, 2010). HIPAA was written to provide peace of mind for consumers and although it cannot entirely stop people from accessing medicals records, it will punish those who are found guilty.

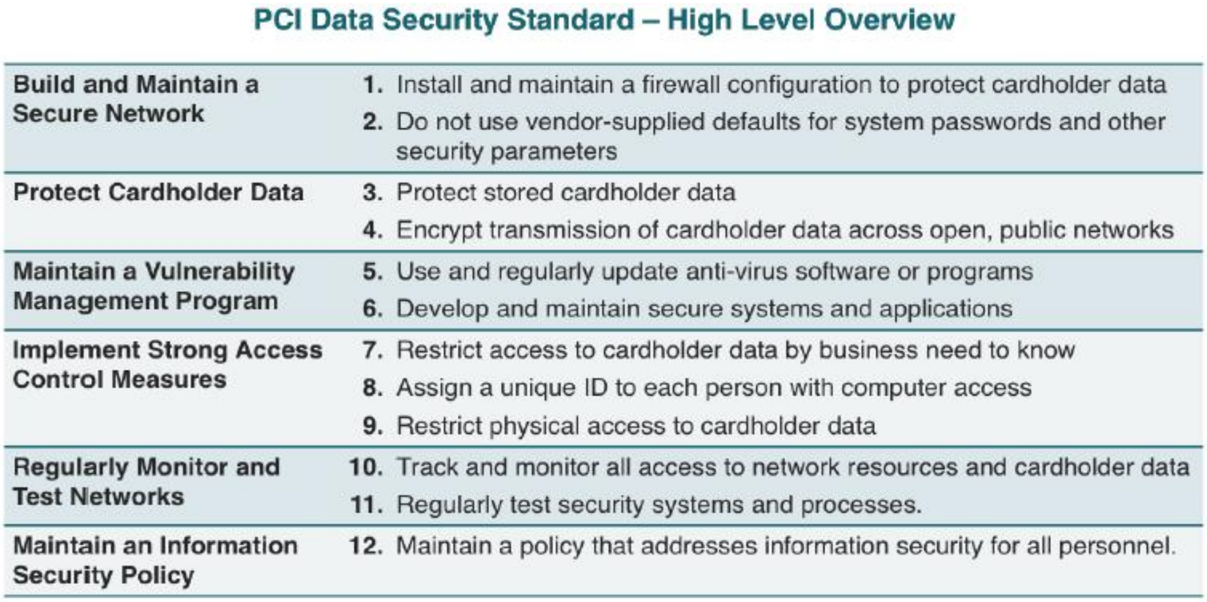
Communications Decency Act (1996)

Section 230 paragraph C of the Communications Decency Act provides “protection for “Good Samaritan” blocking and screening of offensive material” (Legal Information Institute). This portion of the law says that “no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider” (Legal Information Institute). Practically speaking, this provision gives immunity to information content providers and interactive computer services from liability due to what users post on their websites. This was reaffirmed in the case Zeran v. America Online Inc., in which AOL (America Online) was deemed not liable for a defamatory statement posted on one of its online message boards (Zeran v. America Online Inc., 1997).

Payment Card Industry (PCI) Data Security Standard (DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is the method through which the Payment Card Industry group, made up of executives from American Express, Discover, JCB International, MasterCard Worldwide, and Visa Inc., makes sure anyone involved in payment card processing abides by certain rules to ensure maximum data security of customer’s information (PCI Security Standards Council LLC, 2010). PCI DSS is applicable if a primary account number is stored, processed or transmitted during a transaction and requires the protection of all physical and virtual system components such as: servers, applications and routers (PCI Security Standards Council LLC, 2010). Certain sensitive authentication data, including but not limited to, full magnetic stripe data, card verification codes and values (CAV2, CID, CVC2, CVV2), and PINs and PIN blocks, cannot be stored after it is authorized even if the data is encrypted (PCI Security Standards Council LLC, 2010). As it relates to CC, PCI DSS states that any "shared hosting [provider] must protect the [company who is outsourcing]'s hosted environment and data" (PCI Security Standards Council LLC, 2010). Although the rules for CC providers' compliance are very similar, they are not identical to those who actually accept payment cards (a table of CC provider's rules for compliance can be found in Appendix A – Hosted Service Provider PCI DSS Regulations). Fines for failing to comply with PCI DSS range between $5,000 and $100,000 per month (PCI Security Standards Council LLC, 2010).

Compliance with PCI standards is one of the most vital parts to any business that accepts payments from debit and credit cards. The most infamous failure to comply with PCI standards is the TJX Companies Inc. failure between July 2005 and December 2006 (Vijayan, 2007). During a lawsuit between TJX and major banks, which in most cases were required to pay for the fraudulent charges customers reported, the banks claimed that TJX had failed to comply with 9 of the 12 PCI standards, see Figure 2 (Vijayan, 2007). During the 18 months in which the intrusions took place, approximately 94 million accounts had their data compromised (Vijayan, 2007). This incident was a wakeup call to most merchants and consumers that their credit card information is continually under attack and without proper safety measures in place a transaction using a credit or debit cards is extremely risky.



PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

Figure 2 – PCI Data Security Standards (PCI Security Standards Council LLC, 2010)

The aforementioned consumer privacy laws must be followed in the United States by CC providers. One difficulty that will certainly be encountered by CC providers is the legal mess that ensues when they host information in foreign countries - these providers must also follow the laws of that country. For example, Amazon S3 offers to host data in servers in the United States, Ireland, Singapore and Japan and must make sure that if data from an American company is transmitted from the United States to Japan for storage, that consumer protection laws are followed in both the United States and Japan (Amazon Web Services). CC providers must take special care that they follow the myriad consumer privacy laws in each applicable country, or face stiff penalties when they are found to be in violation.

Various Laws Regarding Illegal Material and Copyright Infringement

In addition to the preceding laws regarding consumer privacy, there are a number of laws that can affect the level of privacy a consumer can have. The first of these is the Digital Millennium Copyright Act of 1998, which makes illegal the distribution and production of materials intended to bypass digital rights management measures that protect copyrighted works (The Digital Millennium Copyright Act Of 1998). Another equally important piece of legislation is the United States Code Title 18 §2251, 2252, 2256 and 2260 concerning the production, distribution, reception, and possession of an image of child pornography, which makes it illegal to take part in any of the listed actions (US Department of Justice). If any such material as discussed in these laws is found to be in your possession or in use by a CC provider on your behalf, such as using Amazon S3 to store pirated movies, music and images for example, the government has the right to seize this material and charge the user with a crime. Therefore, not only must consumers be mindful of what is kept on their computers, but CC providers must also make note in their service agreements that should any of this material be found in use with their services, they will freeze the accounts of the user and fully cooperate with the proper authorities.

V. Privacy

Any discussion of information security cannot be complete without a section on privacy. Prior to the digital revolution, the definition of privacy was traced to Samuel D. Warren and Louis D. Brandeis (1890), who said "privacy is the right to be left alone." However, it has since morphed into "the right that a user is informed of how the information about them is being used". As was best said by Michael Whitman and Herbert Mattord (2010), "privacy as a characteristic of information does not signify freedom from observation, but in this context, privacy means that information will be used only in ways known to the person providing it." This raises a major concern for any computer user, especially those in the business setting: What if none of my information is protected?

The answer to this problem is one that is frequently changing in the legal arena, but currently it is most agreed upon that the content of a user's information is protected while the context is not. The belief that content, the actual substance of a message, is protected speech, while context, the details about a message such as a phone number, is not, comes from the case *Smith v. Maryland* (1979). In this case the police, without a warrant, installed a pen register, a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released, on the telephone line of a suspected burglar at the office of the telephone company to discover if he was indeed the caller who was harassing the victim via phone and had, over the phone, admitted to burglarizing her home (Smith v. Maryland, 1979). The burglar was found guilty but appealed on the grounds that the police had violated his 4th Amendment Rights. The case was appealed all the way to the Supreme Court where the court opined that his rights were not violated "for pen registers do not acquire the contents of communications", but that "they disclose only the telephone numbers that have been dialed" and that "neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers." (Smith v. Maryland, 1979).

The use of this case as precedence can cause worry for companies and individuals because of the sole protection of content. As this relates to business, companies who outsource - contract with another company to provide a service - their email, such as using Google Apps, need to have their legal team write up an agreement to include the protection of context as well as content prior to the start of the relationship. This document should be closely related to a non-disclosure agreement, stating what the acceptable use is for each party involved. In this pseudo-non-disclosure agreement, the CC provider should be prohibited from disclosing the amount of data that is moved (the number of emails) or when/where the data moved to (who the recipients of the emails are and where these recipients are located).

VI. Gaps in Security

The first serious gap in security pertains to risks within some small businesses. Most small businesses do not have the capital to employ a full time IT staff or have an Information Security department, leaving an ever expanding role to most likely one employee. This presents a problem because compliance with all regulations, especially PCI and HIPAA, are left to one person who can easily be overwhelmed by the number of tasks to be accomplished or not be knowledgeable enough to protect the company's systems. Both of PCI and HIPAA enforce strict penalties when the rules are violated; companies found to be in violation of PCI standards can face fines of up to $25,000 per day (PCI Security Standards Council LLC, 2010), while violation of HIPAA can land an individual in jail (Dimick, 2010). Although most small businesses do not store credit card information and therefore under PCI Compliance do not need to have the same security standards as those who do, a recent attack against roughly 150 Subway franchises shows just how easily it was for hackers to gather customer's credit card information (Gallagher, 2011). The franchises failed to use the software provided to them by the corporate IT team to secure their POS systems, allowing the hackers to use readily available software to plant malware on the POS systems to monitor credit card transactions (Gallagher, 2011). The franchises that were affected blatantly disregarded the security processes and procedures given to them by corporate IT which requires two-factor authentication to allow access for remote systems, thus easily allowing the hackers to gain entry to their systems (Gallagher, 2011). The reason for each franchise not complying with the security standards is unknown, but it is not without reason to suspect ignorance and apathy to be leading factors. The ease with which hackers gathered the information provides an example as to why it is vital for small businesses to take protective measures and comply with the most rigorous PCI standards (Gallagher, 2011).

Another troublesome gap in security is the commonly held false assumption that most large CC companies operate on a large enough scale that they can employ subject experts on security and not need to worry about hacks into their systems. However, this is not true at all; some of the largest and most sophisticated hacks have come against the world's largest companies! One of the most infamous breaches involving a CC provider is that of the Aurora attack against Google et al. in December of 2009 to January of 2010 (Fitzgerald, Dennis, & Durcikova, 2011). Even though Google is one of, if not the, largest internet-based companies, they were hacked using one of the most sophisticated hacks ever seen against a commercial industry company (Zetter, 2010). In addition to stealing information about certain Google accounts, the hackers were looking for the life blood of online companies: their source code (Zetter, 2010). The hackers were successful in stealing both the source code and information about specific users (the users whose information was stolen are known activists focusing on human rights cases in China) (Zetter, 2010). The attack is blamed on a group in China with the backing of a government organization due to the size and sophistication of the hacks (Zetter, 2010). Those who use CC resources to store their sensitive or private information, be it emails or valuable company documents, must be aware of the inherent risks with transferring the responsibility of maintaining data to a CC provider. Data has become the new currency of the internet and criminals will stop at nothing to get their hands on as much data as possible.

The Subway and TJX cases mentioned earlier raises another problem about CC and information security: the vulnerability of the transmission of data. In the Subway case, unsecured remote access allowed hackers to gain access to the data (Gallagher, 2011), while TJX had unsecured wireless networks allowing hackers to breach their systems (Vijayan, 2007). In both these examples the information was stolen during transmission, so there was nothing the CC providers could do to stop the theft. However, there is a way to make a best effort to protect all data so that it will be secure during transmission. Encryption is the key to data protection. A connection over the internet can be secured using SSL (Secure Socket Layer) protocol or a VPN (Virtual Private Network) with encryption, while the data itself can be encrypted by using symmetric or asymmetric cryptography.

VII. Conclusion

The findings in this paper lead to two basic rules that all companies who use CC services should abide by: encrypt any private data (at rest or in storage) that are to be transmitted and develop a comprehensive non-disclosure agreement with the CC provider. Although the findings can be boiled down to two seemingly simple takeaways, the implementation of these is not as simple.

Encryption is something that has become essential for all companies, especially those who use CC services. There are four different types of data which a user must make sure is secure: data at rest, data in motion, data in use, and data disposed. The two types of data that most concern CC are data at rest and data in motion. Data at rest, also known as data in storage, is best exemplified by data stored in a database, on a laptop or desktop and on an external hard drive or USB flash drive. There are three basic ways to protect data at rest: full disk encryption, virtual disk or volume encryption, and file/folder encryption (Scarfone, Souppaya, & Sexton, 2007). Full disk encryption occurs when all of the data contained on a hard drive is encrypted (Scarfone, Souppaya, & Sexton, 2007). When the entire hard drive is encrypted any user attempting to make use of the hard drive must successfully authenticate before gaining access to the drive; this means a user will have to enter a password for the hard drive to even boot up. This is the most complete way of protecting a hard drive, but can be the most aggravating because of the need to authenticate to boot the computer to perform even simple functions. Virtual disk encryption is attained by encrypting a container, which is a collection of files and or folders of data (Scarfone, Souppaya, & Sexton, 2007). Virtual disk encryption is used so that only a certain group of data is encrypted such as a container made up of sensitive financial information. Volume encryption occurs when a collection of containers aggregated together in a logical volume are encrypted (Scarfone, Souppaya, & Sexton, 2007). The most common logical volumes are the boot, system and data volumes on a typical computer, any of which can be encrypted using volume encryption, with the data volume as the most likely volume to be encrypted. The final type of encryption for data at rest is file or folder encryption. File/folder encryption is the smallest level of encryption that can occur made up of single files or folders, such as encrypting a My Documents folder or a sensitive memo file (Scarfone, Souppaya, & Sexton, 2007). For all of these ways to encrypt data, the best recommended practice is to use single-key encryption with AES because of its strength and speed, see Appendix B – Cryptography for details (Scarfone, Souppaya, & Sexton, 2007).

Data in motion, like data at rest, needs to be encrypted. Samplings of data that are considered data in motion and therefore needs to be encrypted are email messages, credit card numbers and even electronic medical records. Because of the stiff penalties imposed by HIPAA for electronic medical records and PCI for credit card information companies need to make sure the information they are sending over their intranet, a network that is not connected to the outside world, or through the Internet is protected. The best practice for encrypting data in motion is to use public key encryption, discussed in Appendix B – Cryptography (Fitzgerald, Dennis, & Durcikova, 2011). Two common methods of protecting the transmission itself, including the data in motion, are Secure Socket Layer, SSL, protocol or a VPN with encryption, both discussed in Appendix B – Cryptography.

As was mentioned in the privacy section, creating a specific security agreement, in essence a non-disclosure agreement in regards to the ownership of data, with the chosen CC provider will give the client maximum legal protection as well as grounds for recourse if the terms of the agreement are violated. This agreement should say that the CC provider cannot disclose data without prior approval from the client. In addition, the CC provider cannot disclose the content and/or context of any of the data belonging to the client. In addition to being covered on a legal basis, the client will be able to tell its customers that their data will not, under the terms of the agreement, be read or traced.

Given the rate at which companies are adopting cloud computing, there is little chance that laws can be made in time to address all of the issues that arise with a technology that has so many uses. For this reason, companies and consumers must be proactive in protecting their data so that laws can be created to fill in the gaps previously discussed. I believe that the laws still to be created should focus not only on the protection of the content, but also on the context of all data in storage and transmission. It is uncertain what these future laws will protect, but by every stakeholder taking steps to protect itself they can substantially lessen the risk of embarrassing and potentially costly leaks of data.

Bibliography

Smith v. Maryland, 78-5374 (U.S. Supreme Court June 20, 1979).

Zeran v. America Online Inc., 97-1523 (Fourth Circuit Court of Appeals July 7, 1997).

Amazon Web Services. (n.d.). Retrieved October 17, 2011, from Amazon.com: http://aws.amazon.com/

American Medical Association. (n.d.). *HIPAA Violations and Enforcement.* Retrieved April 9, 2012, from American Medical Association: http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page

Amrhein, D., & Quint, S. (2009, April 08). *Cloud computing for the enterprise: Part 1: Capturing the cloud*. Retrieved September 18, 2011, from IBM.com: http://www.ibm.com/developerworks/websphere/techjournal/0904_amrhein/0904_amrhein.html

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., et al. (2010, April). A View of Cloud Computing. *Communications of the ACM, 53*(4), 50 - 58.

Bhardwaj, S., Jain, L., & Jain, S. (2010). Cloud Computing: A Study of Infrastructure as a Service (IaaS). *International Journal of Engineering and Information Technology, 2*(1), 60 - 63.

Cloud Computing | Oracle. (n.d.). Retrieved October 17, 2011, from Oracle.com: http://www.oracle.com/us/technologies/cloud/index.html

Cloud Computing | Productivity Tools | Cloud Hosting | Microsoft Cloud. (n.d.). Retrieved October 17, 2011, from Microsoft.com: http://www.microsoft.com/en-us/cloud/default.aspx#tab1-small

Department of Homeland Security/Office for Civil Rights and Civil Liberties. (n.d.). *Electronic Communications Privacy Act of 1986*. Retrieved March 26, 2012, from Justice Information Sharing: http://it.ojp.gov/default.aspx?area=privacy&page=1285

Dimick, C. (2010, April 29). *Californian Sentenced to Prison for HIPAA Violation*. Retrieved February 20, 2012, from Journal of AHIMA: http://journal.ahima.org/2010/04/29/californian-sentenced-to-prison-for-hipaa-violation/

Fitzgerald, J., Dennis, A., & Durcikova, A. (2011). *Business Data Communications and Networking* (11th ed.). Hoboken, NJ: Wiley.

Gallagher, S. (2011, December 21). *How hackers gave Subway a $3 million lesson in point-of-sale security*. Retrieved January 13, 2012, from ARS Technica.com: http://arstechnica.com/business/news/2011/12/how-hackers-gave-subway-a-30-million-lesson-in-point-of-sale-security.ars

Google Apps for Business. (n.d.). Retrieved October 17, 2011, from Google.com: http://www.google.com/apps/intl/en/business/index.html

IBM Cloud Computing: Cloud Infrastructure. (n.d.). Retrieved October 17, 2011, from IBM.com: http://www.ibm.com/cloud-computing/us/en/cloud-infrastructure.html

IBM Corporation. (n.d.). *IBM Cloud Computing - Overview*. Retrieved March 24, 2012, from IBM.com: http://www.ibm.com/cloud-computing/us/en/index.html

Legal Information Institute. (n.d.). *18 USC § 2511 - Interception and disclosure of wire, oral, or electronic communications prohibited*. Retrieved November 28, 2011, from Legal Information Institute: http://www.law.cornell.edu/uscode/text/18/2511

Legal Information Institute. (n.d.). *United States Code: Title 47, 230 Protection for the private blocking and screening of offensive material*. Retrieved January 23, 2012, from Legal Information Institute: http://www.law.cornell.edu/uscode/47/230.html

Mell, P., & Grance, T. (2010). The NIST Definition of Cloud Computing. *Communications of the ACM, 53*(6), 50.

Microsoft Corporation. (n.d.). *Office 365*. Retrieved November 1, 2011, from http://www.microsoft.com/en-us/office365/online-software.aspx

Microsoft Corporation. (n.d.). *Windows Azure Platform*. Retrieved November 1, 2011, from http://www.microsoft.com/windowsazure/

Mullan, E. (2010). Many Still Cloudy on the Definition of Cloud Computing. *EContent*, *33*(1), 12-13.

Parks, R., & Harvey, J. (2008). *Cloud Computing: What to Ask When the Clouds Roll In.* http://www.hunton.com/files/Publication/d31b869a-1b7d-4422-aeb5-d4569490b029/Presentation/PublicationAttachment/35e40e83-73ef-4a1d-8ee0-0078d3ebafe3/Cloud_Computing.pdf: Hunton & Williams LLP.

PCI Security Standards Council LLC. (2010, October). *PCI Security Standards Documents.* Retrieved November 15, 2011, from PCI Security Standards Council LLC: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

Scarfone, K., Souppaya, M., & Sexton, M. (2007, November). *Guide to Storage Encryption Technologies for End User Devices.* Retrieved February 20, 2012, from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

Software & Information Industry Association. (2001). *Software As A Service: Strategic Background.* Software & Information Industry Association.

The Digital Millennium Copyright Act Of 1998. (n.d.). Retrieved March 26, 2012, from http://www.copyright.gov/legislation/dmca.pdf

US Department of Health & Human Services. (n.d.). *Health Information Privacy*. Retrieved March 26, 2012, from US Department of Health & Human Services: http://www.hhs.gov/ocr/privacy/

US Department of Justice. (n.d.). *Child Exploitation and Obscenity Section (CEOS)*. Retrieved November 15, 2011, from US Department of Justice: http://www.justice.gov/criminal/ceos/

US Department of Justice. (n.d.). *Child Exploitation and Obscenity Section (CEOS)*. Retrieved November 15, 2011, from US Department of Justice: http://www.justice.gov/criminal/ceos/citizensguide_porn.html

Valacich, J. S., George, F. J., & Hoffer, A. J. (2012). *Essentials of Systems Analysis and Design.* Boston: Pearson.

Vijayan, J. (2007, October 26). *TJX violated nine of 12 PCI controls at time of breach, court filings say*. Retrieved January 21, 2012, from Computerworld Inc.: http://www.computerworld.com/s/article/9044321/TJX_violated_nine_of_12_PCI_controls_at_time_of_breach_court_filings_say

Warren, S. D., & Brandeis, L. D. (1890, December 15). The Right to Privacy. *Harvard Law Review*, *4*(5), 193-220.

Whitman, M. E., & Mattord, H. J. (2010). *Management of Information Security*. Boston: Course Technology.

Zetter, K. (2010, January 14). *Google Hack Attack Was Ultra Sophisticated, New Details Show*. Retrieved February 8, 2012, from Wired: http://www.wired.com/threatlevel/2010/01/operation-aurora/

Appendix A – Hosted Service Provider PCI DSS Regulations

Source: PCI DSS Data Security Standards

Requirements	Testing Procedures
A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. **Note:** Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.	**A.1** Specifically for a PCI DSS assessment of a shared hosting provider, to verify that shared hosting providers protect entities' (merchants and service providers) hosted environment and data, select a sample of servers (Microsoft Windows and Unix/Linux) across a representative sample of hosted merchants and service providers, and perform A.1.1 through A.1.4 below:
A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	**A.1.1** If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example: No entity on the system can use a shared web server user ID. All CGI scripts used by an entity must be created and run as the entity's unique user ID.
A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only.	**A.1.2.a** Verify the user ID of any application process is not a privileged user (root/admin).
	A.1.2.b Verify each entity (merchant, service provider) has read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.) **Important:** An entity's files may not be shared by group.
	A.1.2.c Verify that an entity's users do not have write access to shared system binaries.
	A.1.2.d Verify that viewing of log entries is restricted to the

	owning entity.
	A.1.2.e To ensure each entity cannot monopolize server resources to exploit vulnerabilities (for example, error, race, and restart conditions, resulting in, for example, buffer overflows), verify restrictions are in place for the use of these system resources: • Disk space • Bandwidth • Memory • CPU
A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	**A.1.3** Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment: Logs are enabled for common third-party applications. Logs are active by default. Logs are available for review by the owning entity. Log locations are clearly communicated to the owning entity.
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	**A.1.4** Verify the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise.

Appendix B – Cryptography

Good encryption is one of the best ways a company can protect its data, assuming that they key used is of adequate length and is protected in the real world. One important note about encryption is that it is illegal for anyone to encrypt a message with a key strength of more than 64 bits because with a key in excess of 64 bits the encryption becomes too difficult for the government to break in case it is needed.

Single-Key encryption (also known as Symmetric Encryption) consists of two parts, the algorithm and the key, used in combination to disguise the information. When using single key encryption, each user must have a copy of the same key so that the information can be encrypted by one user, and decrypted by the other. There are multiple different levels of protection provided by single key encryption with AES (Advanced Encryption Standard) as the current best used practice. The disadvantage of single-key encryption is that each user must know the key and if the message is being transported then it will need to include the key, which is a very risky proposition.

Public-Key encryption also consists of two parts, the algorithm and the key. However, in public-key encryption there are two types of keys needed, a public key and a private key. Each user has a public key and a private key. The process of using public-key encryption works like this: User A has a public-key and a private key and wishes to send a message to user B. So user A will look up user B's public-key in an online directory, usually done automatically if using encryption software, and will then encrypt the message using this public key. Once the data is encrypted, it cannot be decrypted with the public key, user B's private key is the only way to decrypt the data. User A is then free to send the encrypted message to user B, which user B will then decrypt using his/her private key, revealing the original message.

Another useful tool for securing a transmission is the use of Secure Socket Layer, SSL, when transmitting sensitive information over the internet. SSL is used by most major web retails today especially those who take bank card information over the internet and those who have web-based email.

A Virtual Private Network, VPN, is a secure connection used for a variety of business functions. When using a VPN, a secure connection is created between the user's computer and the computer that initiated the connection. A VPN is most often used when an employee travels to a foreign connection and the company the employee works for wants to make sure the employee has a secure way to do such things as check email and access documents hosted on the company's servers.

Other resources:
A list of encryption software for PC's: http://download.cnet.com/windows/encryption-software/

The National Institute of Standards and Technology's webpage has a plethora of useful information: http://csrc.nist.gov/groups/ST/toolkit/index.html

More information on the legality of using encryption:
http://www.bis.doc.gov/encryption/default.htm