Cloud Computing

What are the significant security threats that might impede its adoption?

Felix Paulino Rante

A dissertation submitted to the University of Dublin
In partial fulfillment of the requirements for the degree of
MSc in Management of Information Systems

2 September 2013

Declaration

I declare that the work described in this dissertation is, except where otherwise stated, entirely my own work, and has not been submitted as an exercise for a degree at this or any other university. I further declare that this research has been carried out in full compliance with the ethical research requirements of the School of Computer Science and Statistics.

Signed: _____

Felix Paulino Rante

31 August 2013

Permission to lend and/or copy

I agree that the School of Computer Science and Statistics, Trinity College may lend or copy this dissertation upon request.

Signed: _____
Felix Paulino Rante
31 August 2013

Acknowledgements

I would like to thank all my professors and the entire academic staff of the School of Computer Science and Statistics for their help and support throughout the course and dissertation. Special thanks to my supervisor Anthony Niland for all the valuable advice and assistance extended throughout.

I am also grateful to generous organizations such as Verizon Enterprise, Veracode, WhiteHat, Imperva, Ponemon Institute and many others who willingly shared the results of their studies. To all friends and colleagues who had extended a helping hand and shared their knowledge and expertise thank you!

Finally, I owe my wife, Annie Lou and my daughters, Saoirse and Roisin, a lot for all the support and inspiration, without them, this dissertation would not have been possible.

Abstract

Cloud computing, a $131 Billion industry (Gartner, 2013), is undeniably a significant topic today. Its influence can be observed from the way people store data to the way enterprises deploy and manage enterprise applications. Software as a Service (SaaS), which is the most popular layer, is also considered to be the most vulnerable layer of cloud computing. This layer delivers services, software applications, over the same cyberspace where cybercriminals operate; hence, security considerations remain critical. A review of security reports such as the Verizon's Data Breach Investigation, Ponemon Institute's Cost of Cybercrime, Trustwave global security reports, among others, show that security is a priority action. This study aims to reveal the technical security issues of SaaS based solutions. It looks at the most prevalent vulnerabilities and the commonly exploited ones within the cyberspace security environment. The study adopts both the positivist and the interpretivist philosophies employing quantitative and qualitative approach in data gathering.

The data show that while cloud adoption is on upward trend, it is slowing. Cloud users consider security the biggest barrier to cloud. 8 out of 10 widely used web services today possibly have serious vulnerabilities. In some industries, these vulnerabilities remain untouched for up to 342 days, giving hackers a lot of time to exploit them. The most prevalent vulnerabilities on web applications are Cross Site Scripting, Directory Traversal, Information Leakage, and SQL Injection; some of these vulnerabilities also appear to be the most exploited ones. Until application developers/providers are able to deliver vulnerability free applications, cyber-attacks will continue to flourish, and this could affect cloud adoption.

Table of Contents

List of Tables and Figures

1. Introduction

The advancement in networking and telecommunication technologies, as well as development in software technologies, offers many new possibilities. The increased internet bandwidth, for instance, allowed more services to be delivered; likewise the advancement on web technologies enabled application developers/providers to offer more powerful software solutions or services that previously not possible to deliver over the Internet. The confluence of the increasing power of the internet and the innovative development in software technology is what makes cloud based computing possible.

Cloud computing is changing the way people and businesses use computing technology, by combining the power of the internet with the brilliance of software technologies, it introduces a whole new computing paradigm, causing disruptions among enterprises across all industries in the world. For example, Software as a Service (SaaS), a layer of cloud, provides users ready access to software applications such as productivity software like word processing, spreadsheet and presentation (e.g. Microsoft Office 365 for 10.40 Euros/user/per month), no deployment, no installation and maintenance required; the other benefits are, currently, all updates are free; the maintenance and support are now the provider's responsibility; high end desktop machines are no longer needed as the application runs on web browsers, and what's even better is that, companies can easily increase the number of subscriptions as they expand, and if needed change provider or discontinue the subscription. This new computing model offers a lot of advantages that enterprises find difficult to ignore; however, while research reports (Chapter 4) show that many companies have embraced this new paradigm, cloud computing faces one significant challenge: security; InformationWeek and CDW's surveys on the state of cloud computing, show that this concern is shared by those users who have already adopted cloud and the ones who are still in the process of migration.

This study looks at cloud computing security in the context of SaaS.

1.1 Background

Cloud computing is a radical paradigm in the history of computing. It is changing the way people do computing, from the simplest task of storing files, to the most complicated business functions like enterprise application deployment; all have been affected and changed for the better. More advanced and powerful software which previously only available as desktop applications such as word processing, spreadsheet, presentation software, video and image

editing applications, among others, are now delivered as Software as a Service applications. Software developers are now able to focus on their coding job because cloud providers now offer ready to use software development platforms – Platform as a Service (PaaS) -, this saves developers a lot of time configuring servers and all tools required to develop and test their apps. The Infrastructure as a Service (IaaS) offering of cloud providers, on the other hand, helps enterprises to be more agile; this service makes downsizing and expansions easier and more cost-effective as IaaS allows automatic scaling of resources as a need arise, also referred to as the elasticity feature of cloud computing.

With all these new unlocked capabilities, cloud computing is one of the significant developments in computing history, current literature indicates that everyone - cloud users, practitioners and researchers – agree about the greatness of this disruptive technology. However, there is also a consensus that cloud computing is not without a fault: security is cloud computing's biggest challenge.

Because cloud based services, SaaS based solution in particular, are delivered over the Internet, a public network, cloud computing seem to have an intrinsic security problem. As criminals had started to conduct their activities online, the Internet or the cyberspace had become a risky place; this means that cloud computing, a multi-billion dollar business is being run in a risky environment.

This study aims to validate the security worries of cloud users and identify the significant technical issues surrounding SaaS based solutions.

1.2 Importance of the Study

Cloud computing had created a multi-billion dollar industry in just a little more than a decade; many major IT players have targeted the industry launching various cloud based services; Amazon, Google, Microsoft, Apple, Oracle, HP, IBM, among others, are now vying to get a bigger share of the ever growing cloud computing market, which according to Gartner had reached $ 111 Billion in 2012 and was estimated to grow to $131 Billion in 2013.

In terms of the size of the cloud market and its opportunities, it is a significant topic. This study looks at a specific aspect of cloud computing: security. Cloud security is arguably one of the most contentious topic among IT and business strategies today, the question whether to "cloud or not to cloud" depends on the outcome of cloud security vs. cloud advantage debates. Based on research and publications, the issue on cloud advantages has already

been settled; there appears to be general agreement about the potentially tremendous benefits that it offers; it is the issue of cloud security, which this study aims to address.

1.3 The Research Question

While it is not difficult to believe that security issues on cloud do exist, the specific security issues remain in question. Cloud security is everyone's concern but what is the basis of this concern? Are data held or process in the cloud unsecured then why and what's the actual problem?

This is what the study aims to identify; it aims to understand the technical issues surrounding cloud computing on a technical level (application level) and determine the following

- What are the technical vulnerabilities of a SaaS based solutions
- What are the commonly exploited vulnerabilities or attack vectors
- What are the implications of data breaches

1.4 Beneficiaries of the Study

This study is aimed at the application developers but should also benefit the entire cloud computing community. As this study aims to reveal the technical vulnerabilities of cloud based solutions, application developers will learn the most prevalent vulnerabilities on web applications and the commonly exploited vulnerabilities. Application developers and other cloud stakeholders will also understand the following

- Risk, consequences and the cost of data breaches
- The current state of cloud computing adoption
- The current state of cyberspace security.

Specific recommendations on how to improve cloud and the cyberspace security are also proposed.

1.5 Scope of the Study

The study looks at cloud security in the context of SaaS, the discussion on IaaS and PaaS, which appears in some sections, is for the purposes of placing ideas in perspective, additional information and references are offered as a further topic for additional research.

1.6 Chapters Roadmap

The dissertation is divided into 5 chapters and is structured as follows

1.6.1 Chapter I: Introduction

The first chapter provides an overview of the topic; the rationale; relevant background information; the research question, its importance and the target audience; the scope of the study as well as the roadmap of all the subsequent chapters.

1.6.2 Chapter II: Review of Related Literature

Chapter II offers relevant information about cloud computing and security to help establish a better understanding of the subject area. This includes review of current publications, information on data security, SaaS components & its technical environment, and a review and analysis of related studies with supporting data.

1.6.3 Chapter III: Methodology and Fieldwork

The third part explains the research methodology used to undertake the study, the suitability and strengths of the chosen methodologies are argued; the data gathering tools used are enumerated and rationalized; the sampling techniques and the logistics involved are described.

1.6.4 Chapter IV: Findings and Analysis

In this chapter, the summary of all the data from different sources are presented along with the outcome of the analysis on these data. It provides the framework used in the analysis/interpretation of the data and a justification of the results.

1.6.5 Chapter V: Conclusions and Future Work

The last chapter presents the answer to the research question and sub questions. The significant technical security issues of cloud computing are revealed and the possible impact of these issues to the future of cloud computing presented.

2. Literature Review

2.1 Introduction

The influence of cloud computing over how companies conduct business is evident; the statistics (Gartner, 2013) (KPMG, 2013) show that businesses are benefiting from the cost saving features/characteristics of cloud computing and that the adoption is on the upward track; from several hundred million in 2008 (Bloomberg, 2008) to $111 Billion in 2012 all the way to $131 Billion this year (Gartner, 2013). While these numbers are significant, some experts believe that because of cloud security issues, the rate of cloud adoption is slow and that market size is smaller than expected (Chen and Zhao, 2012)

Researchers and security experts (section 2.3.1, page 8) consistently cite security as a significant issue in cloud adoption; the most recent events in the cyberspace seem to support this concern (section 2.3.4, page 12); cyber-attack is on the rise, the volume of data being exposed to cyber criminals has never been greater (Verizon Enterprise, 2013), cybercrimes continue to be costly (Ponemon Institute, 2012), identity theft, corporate espionage and many other illegal activities have continued to flourish.

The goal of this section is to provide substantial information on cloud computing and security including its business case and challenges, latest events in the cyberspace, relevant technical details about this disruptive phenomenon, review of related studies and a short discussion on data security.

2.2 Cloud Computing Hype

The business case of cloud computing cannot be underestimated; Academic professionals, researchers and IT practitioners around the world, more often than not, agree with the benefits that this disruptive phenomenon provides to the business community. Winkler (2011, p. xx) described cloud computing as a “landscape that offers great value and services”; Ken Phelan, the CTO of Gotham Technology Group believe that cloud computing is indispensable because it lowers the cost while increasing productivity (Krutz and Vines, 2010, p. xxii); The Authors of Cloud Computing, Principles and Paradigms, (Buyya, Broberg and Goscinski, 2011, pp. 16-17) likewise provided a list of cloud computing’s desirable features which they claimed to have enabled services that satisfy the expectations of consumers.

The predictions and findings of research organizations and IT business executives seem to agree with what the academics and professionals have been writing about cloud computing. In 2008, when cloud computing was still a several million dollar business, Merrill Lynch's study suggested that it would be a multi-billion dollar in few years (Figure 2.1), Dell's CEO Michael Dell agreed; he stated, "Now it's a several-hundred-million-dollar business, and it will be a billion-dollar business in a couple of years—it's on a tear." (Bloomberg, 2008); they were right, according to Gartner (2013); the cloud market had reached $111 billion in 2012.

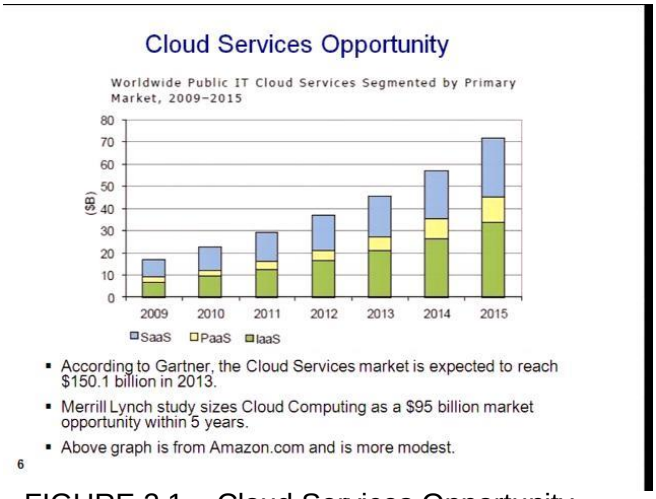


FIGURE 2.1 – Cloud Services Opportunity

Source taken from Harvard University Extension School, 2012, *Cloud Computing and Software as a Service*

A recent survey published by KPMG, entitled "The cloud takes shape Global cloud survey: the implementation challenge", confirms that businesses enjoy financial benefits of using cloud services, the survey shows that 70% of their 674 respondents believe that the cloud is delivering efficiencies and cost savings (KPMG, 2013). Gartner's forecast for 2013 is still positive, stating that public cloud market will grow 18.5 percent in 2013 to the total of $131 billion worldwide, up from $111 billion in 2012 (Gartner, 2013). These findings and positive forecasts are fueling the competition for cloud computing market share; Table 2.1 shows the list of major companies competing for the cloud market.

TABLE 2.1 - Key Players in Cloud Computing Platforms

Company	Cloud computing platform	Year of launch	Key offerings
Amazon. com	AWS (Amazon Web Services)	2006	Infrastructure as a service (Storage, Computing, Message queues, Datasets, Content distribution)
Microsoft	Azure	2009	Application platform as a service (.Net, SQL data services)
Google	Google App. Engine	2008	Web Application Platform as a service (Python run time environment)
IBM	Blue Cloud	2008	Virtualized Blue cloud data center
Salesforce.com	Force.com	2008	Proprietary 4GL Web application framework as an on Demand platform

Source taken from Furht, B. and Escalante, A., (2010) *Handbook of cloud computing*. Springer, Florida adapted from Lakshmanan (2009)

The figures (Figure 2.1) (Gartner, 2013) show that the trend is upward; the question is, is the adoption rate fast, or slow as what some experts claim (Chen and Zhao, 2012)? Is this positive trend going to continue and for how long? Is there anything that could possibly change this trend?

2.3 Cloud Computing Challenges

Despite the overwhelming benefits of cloud computing (Table 2.2) and widespread availability of cloud services from industry leaders, many enterprises still appear to be hesitant about migrating to the cloud. Researchers and industry analysts (section 2.3.1, page 8) consistently cited security and privacy concerns as the most significant barriers in cloud adoption. For example, the KPMG's global study on cloud computing mentioned earlier revealed that the top three concerns about cloud are all data security and related threats (KPMG, 2013).

TABLE 2.2 – Cloud Computing Drivers

Drivers
Pay-as-you-go
Virtual and On-Demand
Agility, Flexibility and Elasticity
Multi-Tenancy
Ease of Implementation
Pooled Resources

Source adapted from KPMG (2011). *The Cloud, Changing the Business Ecosystem.*

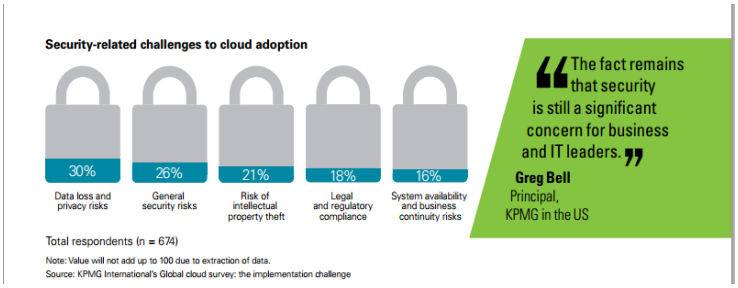


FIGURE 2.2 - Security related challenges to cloud adoption

Source taken from KPMG (2013). *The cloud takes shape Global cloud survey: the implementation challenge.*

Figures 2.2 and 2.3 suggests that security remains a significant concern for users, while more data is needed to be able to quantify the loss opportunity, 30% who had worries about Data Loss and Privacy Risk of migrating to the cloud, alone, is a substantial number, which could be equated to a significant loss for the cloud industry.

2.3.1 Data Security and Privacy Issues in Cloud from International Perspective

The result of KPMG's Global cloud survey (KPGM, 2013) supports the findings of the following researchers.

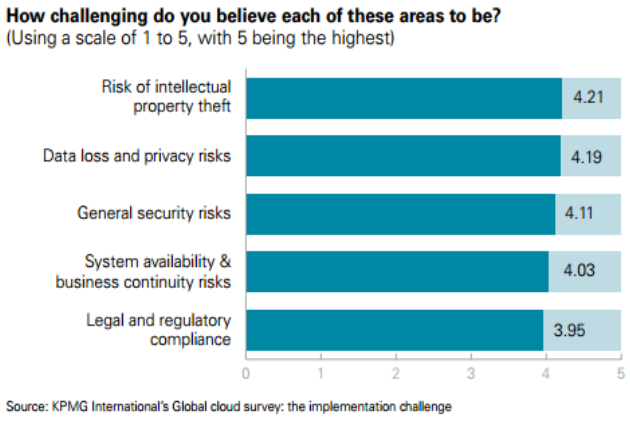


FIGURE 2.3 - Security level of challenge

Source taken from KPMG (2013). *The cloud takes shape Global cloud survey: the implementation challenge.*

Farzad Sabahi (2011), a Faculty of Computer Engineering Azad University Iran, claims that IT organizations have concerns about cloud security which he argued to be due to the data being stored remotely.

A group of researchers from the University of Pune's on the paper they presented to the 2012 IEEE 3rd International Conference on Software Engineering and Services Sciences argued that, despite the potential benefits of cloud computing, security issues and challenges associated to cloud computing is a significant barrier to cloud adoption (Kulkarni, et al., 2012).

Chinese researchers, likewise, believe that the “smaller than expected” [sic] market size of cloud computing is due to cloud computing security concerns, data security and privacy protection issues in particular (Chen and Zhao, 2012).
Mohamed Hamdi, a Tunisian researcher from the Higher School of Communication of Tunis, said that “despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are impeding momentum and will eventually compromise the vision of cloud computing as a new IT procurement model” (Hamdi, 2012). He argued that since the data could be stored anywhere in the world, there are various security and privacy issues that need to be accounted for;

A team of academic researchers from Pakistan also believe that “lack of security is the only hurdle in wide adoption of cloud computing” (Shaikh and Haider, 2011).

European researchers, Meiko Jensen et al. (2009), likewise, argued that before companies could realize the economic benefits of cloud computing, a number of issues particularly the security and trust issues have to be addressed.

University of South Africa’s, Ramgovind Eloff (2010), argued that while cloud computing can change the way people use the Internet in a better way, it poses some security risk that technology adopters need to understand.

2.3.2 Security Assurance from Cloud Vendors

SalesForce, a leading cloud service provider, acknowledges that security and privacy are the most significant obstacles to cloud adoption; the company maintains that in order to gain the trust of users, providers must offer an acceptable level of security and privacy, which either meet or exceed what is achievable for a SaaS based solutions (SalesForce, 2010). Amazon’s paper likewise, states that “Helping to protect the confidentiality, integrity, and availability of our customer’s system and data is of the utmost importance to Amazon Web Services (AWS), as is maintaining customer trust and confidence” (Amazon, 2013). Amazon, undeniably, was able to reflect this commitment on their security white paper, the well-defined security layers and rigidness of all security procedures that Amazon had put in place unquestionably proves its point. Just like Amazon, Google’s commitment to information security is undisputable, aside from the security paper that it releases periodically; the company dedicated two separate URLs that outline its Code of Conduct and Security

Philosophy (Google, 2010). Other service providers are putting the same effort to persuade the business community that the cloud base services that they provide are well secured, and data are substantially protected.

While the overwhelming efforts of cloud providers to assure data security are unequivocal, the sufficiency of these efforts remains in question. The news about the PRISM program – Edward Snowden revelations - of the United States government, does not just damage the reputations of cloud providers involved in the program, but also the entire cloud industry. A survey conducted by the Cloud Security Alliance (CSA) shows that the Snowden incident negatively impacts the US' cloud industry, 10% of the respondent cancelled projects on US-based cloud providers and 56% will less likely use a US-based cloud providers (Cloud Security Alliance, 2013).

Another significant issue that the cyber community, cloud service providers in particular, has to address is the continuing cyber-attacks. Hacking and cyber-attacks have been rampant in the recent years; various hacking organizations/unions arose and some became household names such as Anonymous, Lulz Sec, Anti Sec, Honker Union of China and Portugal's cyber army.

2.3.3 Hackers' Organizations and Cyber-attacks

Despite all the efforts and significant investments that huge multinational companies, internet companies in particular, put up to improve the security of their respective online services, still, many have fallen victims of cyber-attacks. Hackers have recently been more aggressive and seem unstoppable than before, regularly attacking multinational corporations, government and private organizations worldwide.

The group Anonymous which was formed in 2003 and described itself as a hacktivist group, had successfully attacked huge multinational companies such as PayPal, Symantec, MasterCard, Visa, Sony, the US Federal Reserve, Bank of America and many other companies in various continents; even the Vatican and a number of religious organizations such as the church of Scientology were not spared; the group had successfully stolen and leaked user details, passwords and other private information.

The Lulz Security also known as LulzSec - a small group of hackers from its parent group Anonymous – is also on a hacking spree, the group had hit Fox.Com, LinkedIn, Public

Broadcasting Service (PBS), the US Senate, the US Central Intelligence Agency (CIA), the US Federal Bureau of Investigation (FBI), Bank of America, Bank of Portugal, Portugal's National Police, and many other government website.

The group AntiSec, also a subgroup within Anonymous, had successfully attacked the Arizona's Department of Public Safety, websites of the Government of Brazil and Brazil's President, UK based news organization The Sun, and an FBI's contractor ManTech International.

Other hacking organizations from different countries such as Portugal's cyber army have been impacting the security arena, they hacked the Dubai International Airport in April and the Hong Kong Police in May 2013; the group had previously attacked the global financial credit agency, Moody, allegedly due to the agency's decision to downgrade Portugal's credit rating. Honker Union of China was accused of hacking both US and Chinese government organizations; Tables 2.3 and 2.4 shows the most famous hackers and the top 5 most notorious hacker groups according to Telegraph and HackDigital.

TABLE 2.3 - Top 5 Most Notorious Hacker Groups

Group Names	Profile
Masters Of Deception (MOD)	This group was based in New York and founded by Acid Phrea, Scorpion and HAC. They were known for hacking credit cards, Julia Roberts is one of their victims. They had stolen credit card number from AT&T system. The FBI and the Secret service were able to neutralized this group after arresting the members and sent them to jail.
Legion of Doom (LOD)	Lex Luthor, Vincent Louis Gelormine in real life, founded LOD. This group used to proliferate hacking knowledge via different journals. Being the biggest rival of MOD, LOD engaged a net based war, also considered to the Great Hacker War, with MOD and lost.
Milw0rm	Milw0rm became popular after a successful operation against Bhabha Atomic Research Center (BARC), the main nuclear center of India, where they were able to stole experiment reports and emails, and also destroyed 2 of BARC's 8 servers. They were also able to successfully attack various websites such as World Cup, Wimbledon, Hotel Ritz , Saudi Royal Family and Drew Barrymore.
Anonymous	Anonymous is one of the most popular and feared hackers organization today. They were able to hack high profile companies such as PayPay, Symantec, MasterCard, Visa, Sony, the US Federal Reserve, Bank of America just to name a few.
Red Hacker Alliance	This is a Chinese group with about 80,000 members, this group was previously known as China Redhackers, and was held responsible for the attacks on CNN websites in 2008. Honker Union, another hackers group, allegedly joined hands with this group.

Source adopted from Giridhar (2011). *5 Most Notorious Hacking Groups Of All Time*

TABLE 2.4 - Top 5 Most famous hackers

Names	Profile
Kevin Mitnick	Mitnick, arguably the most famous hacker alive, was described by the US Department of Justice as "the most wanted computer criminal in United States history". Some of his victims were Nokia, Fujitsu and Motorola. Mitnick was arrested by FBI in 1995 and was only handed five year prison sentenced for entering a plea-bargain agreement.
Kevin Poulson	Kevin shot to fame after his successful operation against the Los Angeles radio station KIIS-FM, he hacked the radio station to win a competition for a Porsche. His operation against the federal investigation's database is what put him under the radar of authorizes, he was sent to prison and became journalist after his released.
Adrian Lamo	Adrian, also known as the "homeless hacker" became famous after he successfully tampered and added his name to the New York Times' expert database. He currently works as a journalist.
Stephen Wozniak	Apple's co-founder, Stephen, built a device called 'blue boxes', as this device allows free long distance phone calls he allegedly use it to call the pope in Rome. He is considered a white-hat hacker and later on built the Apple Computer with his friend Steve Jobs.
Loyd Blankenship	Loyd shot up to fame after authoring the Hacker Manifesto (The Conscience of a Hacker) which he wrote in 1986. Hacker Manifesto was re-published by Phrack magazine and was turned into a film in 1995.

Source adapted from The Telegraph (2009). *Top 10 most famous hackers*

2.3.4 Cyber-attacks continuing and on the rise

The hacking spree continues, on 25th of June, BBC News Asia (BBC News, 2013) and many other major news organizations worldwide, reported successful cyber-attacks on a number of South Korean websites including the website of the office of the President. According to the Science Ministry of South Korea, the attack caused downtime on several South Korean websites including the Blue house -Presidential Office-. This attack is the latest in a series of attacks on various South Korean organizations which includes: government institutions, banks, broadcast companies, among others. The most previous cyber-attack happened on 20th March where 32,000 computers on six South Korean banks and broadcasters were affected; the attacked caused disruption in banking services. The other attacks happened in 2009 and 2011.

On May 18, Japan Times (Japan Times, 2013) reported that Yahoo Japan suspects that up to 22 million user IDs may have been compromised; this is not the first time a major Japan based company was hit by a cyber-attack, in 2011, Sony admitted that the information such as user names, passwords and birthdates of more than 100 million customers might have been compromised; a month before the successful attack against Yahoo, Japan Aerospace Exploration Agency, said information related to the International Information Space Station may have been leaked when someone tried to hack in to their system.

LivingSocial, the second-largest daily deal company behind Groupon was hit in April; CNN Money (Pepitone, 2013) reported that the attacked possibly exposed 50 million user accounts to the hacker/s. A LivingSocial spokesman said the hackers may have accessed names, email addresses, encrypted passwords and the dates of birth of some of the users.

In March, a London based organization that tracks Internet's spam senders and services known as Spamhaus became target of what security experts from the online security firm Kaspersky Lab described as the largest Distributed Denial of Service (DDoS). According to Reuters (Sandle, Holton and Holden, 2013), the attack which was evaluated at 300 Gigabits per second slowed down global internet services.

Microsoft, Twitter, Facebook and Apple are some of the most high profile internet companies that had fallen victims of hacking in February. The Guardian (Jones, 2013) reported on the 2nd of February, that 250,000 twitter accounts may have been compromised and that hackers may have been accessed personal information including usernames, email addresses and passwords. On the 15th of February, HUFF POST (Smith, 2013) reported that Facebook's internal computer network was breached in what Facebook described as a "sophisticated attack"; the company, however, said that no user data was compromised. Four days after, Apple said they were hacked too, according to a CNN (Kelly, 2013) 19th February report Apple said the breach is due a vulnerability on a java software plug-in; the company stressed that no data were exposed. Microsoft's turn took place three days after, on the 22nd of February, HUFF POST (Reuters, 2013) reported that Microsoft was hacked and that the intrusion is similar to Apple and Facebook attacks; the company said there was no evidence of customer data being exposed.

In January, various US banks including the banking giant HSBC, Capital One were hit by massive cyber-attacks, causing dozens of online banking sites' slowdown and/or downtime. According to the New York Times (Perlroth and Hardy, 2013), the scale of the attack has convinced the US government and security researchers that the attacks were the work of Iran.

Some of the most high profile cyber-attacks in 2012 include LinkedIn attack which according to USA TODAY (Foley, 2012) possibly compromised 6.5 million user accounts; the attack on

Sony which according to the China Post (AFP, 2012), hackers were able to steal information of hundreds of Sony's mobile unit clients; the attack on Sony PS3 unit which according to Forbes (Strauss, 2012) exposed a security key that could possibly make all existing consoles capable of decrypting current and future games. These are just some of the major cyber-attacks in 2012; the Hackmageddon website (http://hackmageddon.com) which tracks cyber hacking activities around the world provides hacking timeline and other cyber-hacking information.

It is a significant concern that a small group of hackers are able to penetrate the networks and databases of top corporations. Large enterprises such as Yahoo and Sony, for example, have tons of IT security professionals; these companies have the best security equipment to protect their systems; for these organizations to fall victim of cyber-attacks from a small group of hackers who might be operating in a bunker or a garage is unimaginable. This raises a question that if these multi nationals get hacked what could possibly a small cloud service provider or even a major cloud player can do to assure data security and privacy?

The next section provides some technical background/information about cloud computing to help better understand the cloud architecture, its business case and the security issues surrounding it.

2.4 Cloud Computing Background

2.4.1 What is Cloud Computing

Perhaps the most comprehensive and highly quoted definition of cloud computing is the one coined by Peter Mell and Tim Grance of the National Institute of Standards and Technology (NIST), which reads as follow:

"Cloud Computing is a model for enabling 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. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models", (Krutz, R. and Vines R, 2010, p2). Table 2.5 offers various definitions of cloud computing.

TABLE 2.5 - Other Definitions of cloud computing

Wikipedia	n/a	Cloud computing is Internet- ("cloud-") based development and use of computer technology ("computing"). In concept, it is a paradigm shift whereby details are abstracted from the users who no longer need knowledge of, expertise in, or control over the technology infrastructure "in the cloud" that supports them. It typically involves the provision of dynamically scalable and often virtualized resources as a service over the Internet.
Gartner	Thomas Bittman	Cloud Computing: a style of computing where scalable and elastic IT-enabled capabilities are delivered as a service to external customers using Internet technologies.
AMR Research	Bruce Richardson, and esle	Cloud computing is the next-generation of software as a service, in which a complete software environment is licensed as a subscription from a software vendor and low-cost, secure, and dependable IT hardware infrastructure is 'rented' from a utility-computing provider on demand. ⋯ (omitted) ⋯
THINKstrategies	Jeff Kaplan	A set of web-based tools and services which permit users to acquire computing resources and development capabilities to build or support applications, or perform specific IT functions on a pay-as-you-go basis.
Enterprise Strategy Group	Mark Bowker, Steve Duplessie	'Cloud computing' is nothing more than a service model where business workloads are deployed, transparently executed internally or somewhere on the Internet, and businesses only pay for what they consume. ⋯ (omitted) ⋯
IDC	Frank Gens	Cloud Computing: an emerging IT development, deployment and delivery model, enabling real-time delivery of products, services and solutions over the Internet (i.e., enabling cloud services)
The 451 Group	Dan Kusnetzky, Rachel Chalmers, and else	'Cloud computing' describes a service model that combines a general organizing principle for IT delivery, infrastructure components, an architectural approach and an economic model – basically, a confluence of grid computing, virtualization, utility computing, hosting and software as a service (SaaS).
Forrester/Jupiter Research	James Staten	A standardized IT capability (services, software, or infrastructure) delivered via Internet technologies in a pay-per-use, self-service way.

Source adapted from Woohyun K (2009) *Cloud Computing – is changing a game, Presented at the 2009 Web World Conference*

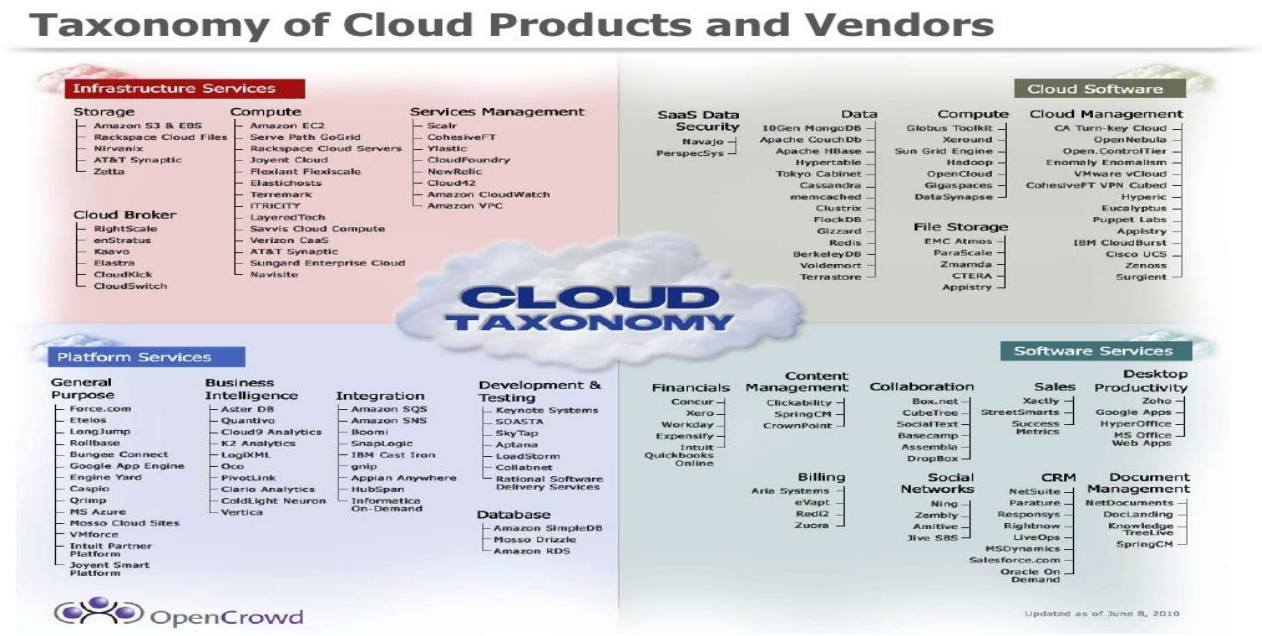


FIGURE 2.4 - Cloud Taxonomy and Vendors

Source taken from OpenCrowd (2010). *Cloud Taxonomy*

As NIST's definition is the one adopted by Irish organizations such as the Irish Software Associations (ISA), Irish Internet Association (IIA), Industrial Development Agency (IDA) the same definition will be used in the study.

2.4.2 Characteristics of Cloud Computing

To put simply cloud computing can be viewed as a computing paradigm that promises to enable companies effectively manage the cost of acquiring and running IT solutions/resources. It is done by providing a flexible platform for resources sharing which has the following five characteristics (Table 2.6) as NIST put it.

TABLE 2.6 – Cloud Computing Characteristics

Characteristics	Description
On-demand self-service	The users are free to configure via a simple interface the services they require.
Broad network access	The cloud services are accessible via high bandwidth communication links, meaning users are able to access the service seamlessly or within an acceptable time frame.
Resource Pooling	The cloud services are supported by large and flexible resource pool that is readily available for allocation as needed. It means resources are well managed and are always available when a need arise.
Rapid Elasticity	This allows the subscriber to automatically purchase resources when needed and offload resources when there is no longer a requirement.
Measured Service	These feature allows dynamic and automatic allocation and monitoring of cloud resources, as the amount of resources utilized is being monitored the customer can then be billed based on the actual service usage.

Source: National Institute of Standards and Technology (NIST)

2.4.3 Cloud Computing Services

Cloud computing provides many benefits to the business such as it lessens the acquisition cost of IT solutions while disburdens enterprises of installation, setup and maintenance activities. Figure 2.5 shows the cloud layers of cloud computing; Table 2.7 offers a brief description of each layer.

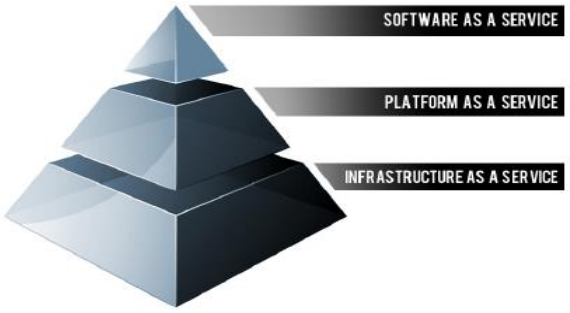


FIGURE 2.5 - Cloud Stacks

Source taken from Rackspace (2012). *Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS*.

TABLE 2.7 – Cloud Computing Services

Cloud Layers	Description
Software as a Service (SaaS)	SaaS provider allows multiple organizations to use a single application remotely using a web browser such as Internet Explorer. This means that the application resides in the provider's server and that the users pay the provider for the services they consume. The provider takes care of everything such as maintaining the server, virus protection, backup among others. The user doesn't have to worry about anything; they simply use the application when they need it. The beauty of using SaaS is that it allows the organization to rapidly expand and downsize anytime in terms of the number of users, meaning companies doesn't have to invest a lot of money on software (e.g. MS Office) upfront in order to operate at the maximum capacity. It also gives companies the ability to switch to other providers more easily and upgrading to the latest version is no longer a problem. SaaS apparently offers a number of benefits, however, SaaS runs on a remote machine which can be located in a different country or continent, the users doesn't have access to the physical machine and has no idea about what's happening in the background while they are doing their work (e.g. typing a confidential memo to shareholders), although data security is normally assured by the provider, it could still be argued that such setup still presents security concerns. SaaS targets the end users and considered to be the top cloud layer. It is perhaps the most widely use cloud service and arguably the most vulnerable layer.
Platform as a Service (PaaS)	PaaS unlike SaaS offers an entire application development environment for Software developers to use. This service, enable software developers to build and deploy application without having to install software development tools on their local machine. To put simply, all the applications required to develop and publish a Web Application to the internet is now made available on demand via a PaaS platform. This allows software development companies to focus on building software leaving the platform configuration and maintenance to the PaaS providers. PaaS providers normally offer pre-configured packages based on OS platform (e.g. Linux Server, Windows Server) or based on CPU cores (e.g. 8 cores, 4 cores). Like SaaS, the subscribers, without having to worry about the technical details, are able to configure the package they need via a simple user interface. This service apparently targets software development companies and is being used by software developers and testers. Apparently PaaS subscribers enjoy the same benefits as SaaS users, it improves the company's productivity while at the same time minimizes cost.
Infrastructure as a Service (IaaS)	IaaS is another layer of cloud which provides businesses access to computing resources such as processing, storage, networks among others. This is like renting physical hardware but instead of having the hardware in the company's premises they are located on the provider's site. Unlike PaaS and SaaS, the users have control over the operating system, storage and application stored in the hardware. This makes a business sense as organizations don not have to invest on dedicated hardware, software and IT personnel upfront. Just like using PaaS and SaaS, employing IaaS allows companies to rapidly expand or downsize their IT resources as and when the need arise.

2.4.4 Deployment Models

One important thing to note about cloud computing is that, a private cloud can be built for the

TABLE 2.8 – Deployment Models

Characteristics	Description
Private cloud	A cloud infrastructure operated for specific organization and maybe deployed on site or offsite. It may be managed by a third party company or the organization's IT department itself
Community cloud	A cloud infrastructure that is shared by several organizations and supports a particular community that has common concerns.
Public cloud	A cloud infrastructure that is open to the general public
Hybrid Cloud	A cloud infrastructure that is made of two or more cloud models, each model remains as is but they are bound together forming a hybrid cloud by standardized or proprietary technology that enable data and application portability.

Source: National Institute of Standards and Technology (NIST)

exclusive used of a company; furthermore, the physical devices could be setup in the company's premises and managed by the company's IT department. While this setup provides companies greater control over security, it is more costly and requires time to implement, which clearly defeats the purpose of cloud computing.

2.5 SaaS Platform Architecture

To be able to deliver software solutions over the Internet a number of software and hardware devices have to be configured. This section provides essential information about the building blocks of SaaS platform.

2.5.1 SaaS Basic Components

A SaaS platform is made up of an Application Server which hosts the application, the database server that hosts the web application's data and the physical server that hosts both the application and the database server. Figure 2.6 shows a simple SaaS platform, in most cases, application and database servers do not reside in the same physical server.

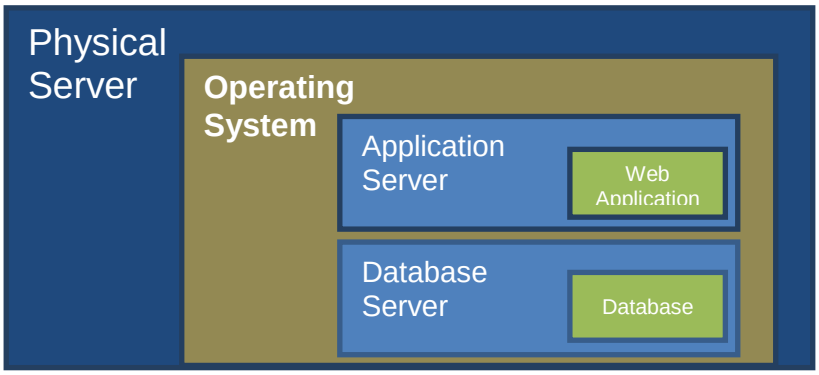


FIGURE 2.6 - SaaS Basic Components

2.5.2 SaaS Architecture

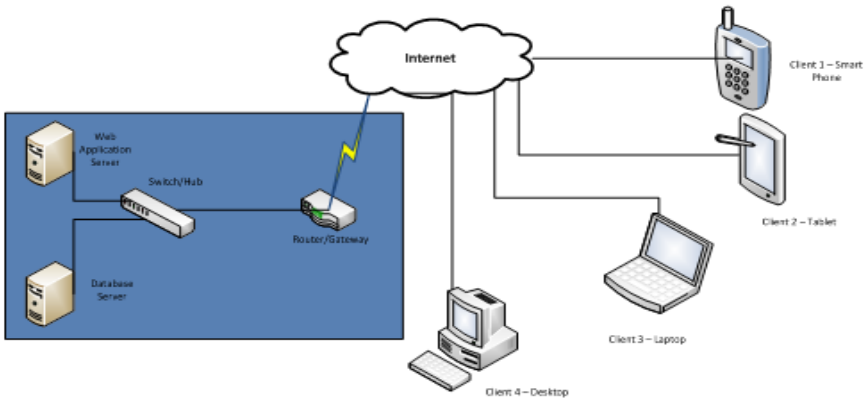


FIGURE 2.7 - SaaS Platform's Basic Setup

Exposing an application over the web has never been easy; the only hardware required is a machine that can run an application and a database server, for low volume traffic both servers could be installed on the same machine. Looking at Figure 2.7, the switch/hub

handles the incoming traffic from the router; the router receives the client requests and forwards them to the appropriate network/switch. The router also takes care of the outgoing response. The web application server hosts all the components of the SaaS platform. The database server is usually a dedicated machine that handles all database related operations and the database file; depending on the amount of data that the database server manages, it could have access to a number of network storage devices. The firewall is responsible for filtering the request; it can be configured to block or modify a request before it forwards it to the target network segment

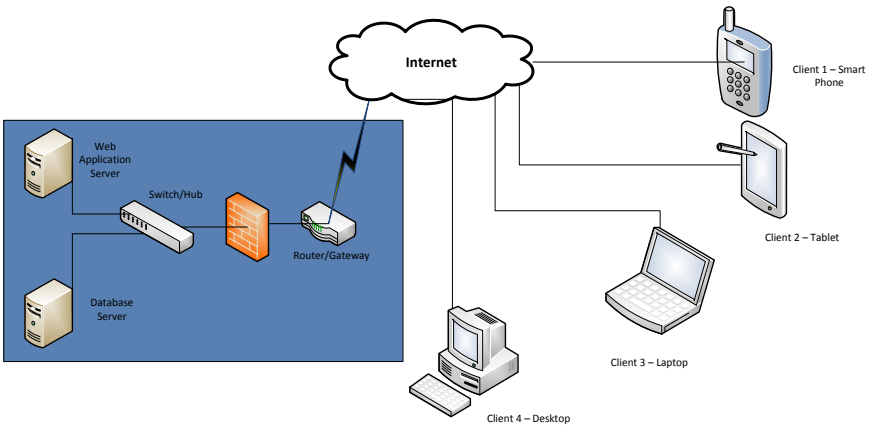


FIGURE 2.8 - Basic SaaS setup with firewall.

2.6 SaaS Platform's Hardware, Software and Protocol

The following sub sections reviews the different components of a SaaS platform.

2.6.1 Hardware Components

TABLE 2.9 – Hardware Components

Components	Description
Server	A server is physical machine/computer that hosts the web application, this computer is the backbone of a SaaS solution It is where the required software such as the OS, Application Server and/or Database Server and other helper tools are installed
Networking Device	a hardware component such as a router or switch that connects a server or workstation to the network. The switch is primarily use to create a network segment
Storage Device	such as internal, external and network attached drives hold both the software and the data. Internal drive is normally part of the server and connected internally, they normally handle system and application software. Network attached (e.g. NAS) and external drives such as USB drive, Tape drive normally hold the data and/or data files.

2.6.2 Software Components

TABLE 2.10 – Software Components

Components	Description
Application Server	is the software that hosts the web application some of the most popular Application Servers are Oracle Weblogic, IBM Webshpere, Microsoft IIS, Apache Server
Database Server	is the software that organizes and stores data to a storage device in a specific format. Most popular database servers offer very powerful tool to administer/manage the entire database including user privilege, database sizing and other configurations; manipulate and retrieve data; as well as import, export, backup and many other maintenance operations.
Firewall	is responsible for filtering both the incoming and outgoing network traffic making sure that the incoming request is safe before its allowed to be routed to the destination and that the outgoing response are valid and appropriate

2.6.3 Protocols

TABLE 2.11 - Commonly used Protocols

Protocols	Description
Hypertext Transfer Protocol (HTTP)	The protocol used by web browsers to communicate to web servers. This is considered to be unsecured because it sends data out without encryption.
Hypertext Transfer Protocol Secure (HTTPS)	The secured version of the HTTP. Using HTTPS requires data to be encrypted before sending it out to the server
File Transfer Protocol (FTP)	Is a network protocol use to transfer file over a TCP based network such as the internet. Like HTTP it transfers unencrypted files over the internet.
Secure File Transfer Protocol (SFTP)	Also known as SSH File Transfer Protocol, unlike FTP, it has secure file transfer capability.
Transmission Control Protocol/Internet Protocol (TCP/IP)	These protocols provide reliable mechanism for the delivery of data packets between programs running on computers connected to an intranet or public Internet.

2.7 Data Security Summary

Alongside the development of sophisticated security platforms such as Firewalls, Anti Malware and other IT security products; is the explosion of sophisticated hacking techniques that have so far successfully penetrated many huge enterprises' well-guarded computer systems. Regardless of the latest hacking techniques employed by the hackers, it is difficult to rationalize why despite all the innovations and developments in the security domain,

companies' security systems are more vulnerable today than years ago. Ken Phelan, CTO of Gotham Technology Group said that an average firm's security system today is less secure than five years ago despite budget increased for this purpose (Krutz, R. and Vines R, 2010, p. xxii). This suggests that hackers had become smarter and poses real threats to the cyberspace community.

This section offers a short discussion on data security.

2.7.1 Data Security over Autonomous Machine

The end point of an attack is usually a machine that can extract data/information from the target data source. Every software application installed in the computer (Figure 2.9) is a potential threat to the system for two reasons, first they could potentially collect information in the background and send it to a remote server; this is particularly applicable to close code OSs, and second these applications could be used by hackers to gain access to the system, this applies to both close code and open source software.

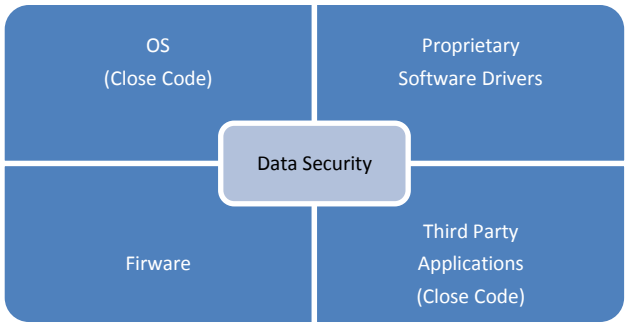


FIGURE 2.9 - Sources of Threats

Close code applications present potential threat because there is no way to verify what they actually do. Many trusted close codes applications such as Java Development Kit (JDK), for example, a widely used programming development platform, according to Apple (Kelly, 2013) and Facebook (Smith, 2013) was the cause of a recent attack against their respective systems; both companies claimed that hackers exploited a bug in Java to execute some malicious code. The bug was immediately addressed, but this proves that any software installed in a machine is a potential threat to the system regardless of the source.

Autonomous machines and any data that it has access are immune from cyber-attacks as apparently the machine is not part of the cyberspace; yet operational, physical and environmental security threats still poses security issues to the data that are stored and/or accessible via autonomous machines.

2.7.2 Data Security over Local Area Network (LAN) and Wide Area Network (WAN)

Unlike autonomous machines, data stored in a computer connected to a network can be accessed remotely and therefore vulnerable to attacks. This section examines the entry attack points on a machine connected to a WAN and/or LAN.

The data security over LAN is considered to be manageable as the system administrators have physical access to all the workstations in the network and therefore able to isolate a compromised workstation easily. In the case of WAN, where only the external IP address of the remote machine is known, the particular workstation that sends a request to a server is hidden from the target server, this makes identification and isolation of the compromised workstation challenging, particularly when dealing with several thousand workstations. Apparently as the number of workstations in the network increases the possible attack entry points and sources of threats also go up. Each workstation correspond to a user, and according to John Vacca in his book Network and System Security, the weakest link in the security is the user training (Vacca J., 2010), he argued that untrained users are the biggest threat to data security, therefore, the bigger the user based a system has; the greater the threat is.

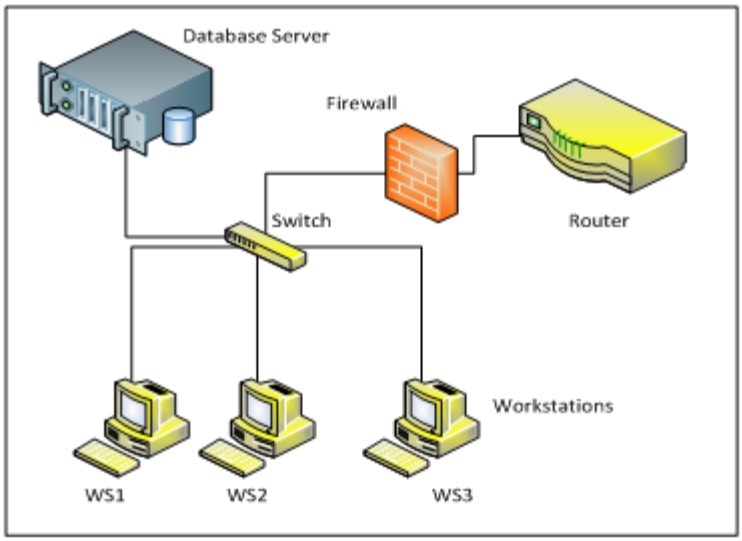


FIGURE 2.10 - Local Area Network

Figure 2.10 shows a sample LAN setup; the server hosts the database; both the data file and the Database Management System software DBMS are accessible from this server; WS1 to WS3 are workstations, have access to Database Server, the Firewall in this setup clearly does not care about what is going on inside the LAN as its only guarding the entry and the exit points. Regardless how secure the network against external attacks the data is still vulnerable to internal attacks, WS1 to WS3 being the possible attack points. However, since network traffic in a local area network can easily be monitored, identifying the compromised machine and isolating it is not much of a problem. Also, a combination of a good network and

local security policies and user training could help minimize this threat, but as hacking techniques becomes more sophisticated, any effort to secure the network won't guarantee absolute security.

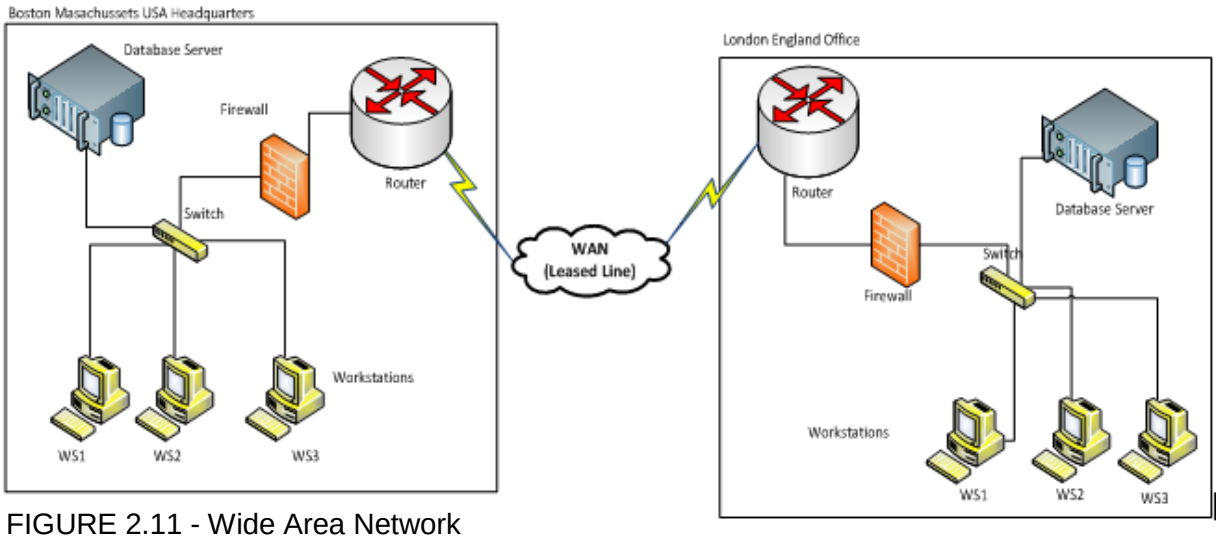


FIGURE 2.11 - Wide Area Network

Figure 2.11 shows a simple WAN setup connecting two LAN's, one located in the USA and the other in the UK. The two LANs are connected via a leased line, so the connection is relatively secured as no one else uses the line except for the company owned workstations. Although this setup is not absolutely secured, it would be difficult for the attackers to hack in; as the line is private, the only way that hackers could gain access is to hack in to the provider's system, which is not an easy undertaking. Just like in LAN, each workstation in a WAN is a possible attack point, and as the number of workstations grows the network becomes more vulnerable.

In summary, applications and resources that are deployed to either LAN or private WAN -using leased lines- is relatively safer. The security becomes questionable when WAN uses the internet as the connection medium; it gets more complicated when both the application and data is migrated to a third party server and are accessed via the Internet. The next section discusses data security over cloud.

2.7.3 Data Security over Cloud

The Internet is open to the public, deregulated and unmonitored; it somehow connects all workstations in the world to each other forming a global network of computers. It has become an integral part of our daily activities; from buying and selling products and services;

socializing with friends, family and professional contacts; advertising products and/or services; online banking, stock market trading, among others; considering all the sensitive personal and financial data that is transmitted over the Internet, it also has become an ideal place for criminals. The Verizon Data Breach Investigation Report (2011), reveals that 50% of reported security breaches in 2010 were due hacking, this was 10% up compared to the 2009 survey, physical attack only accounted 29% which suggests that the preferred medium for cyber-attack is still the Internet.

The benefits of cloud based computing is undeniable; being able to provide enterprises a cost-effective and easy access to applications are compelling business case. However, public network such as the Internet is an unsafe medium to deliver software solutions; the concern about cloud security seems to be a significant impediment to the success of cloud computing. The goal of the study is to identify the significant technical security issues of cloud computing, and understand its impact to cloud adoption.

2.8 Conclusion

2.8.1 Summary of related studies

The various studies reviewed in this section, undoubtedly, contributed a significant amount of knowledge to the field. They offered a good explanation on the different components of cloud computing, and present constructive criticisms and valuable recommendations. However, the majority of these studies tried to cover the entire subject of cloud computing (e.g. all layers such as IaaS, PaaS and SaaS), which affected the breadth of the study and in some case made it look disarray. For example, Meiko Jensen et al. in the paper they presented to the 2009 IEEE International Conference on Cloud Computing, talked about “Technical Security Issues in Cloud Computing”, the paper started with the explanation about cloud computing, the various cloud layers and technologies; they then discussed the different technical issues of cloud computing covering XML signature, Browser security, Cloud Integrity and Binding Issues, and Flooding Attacks; the final part is where they laid out their recommendations. The problem is that security is in itself a substantial topic, and therefore must be well defined in order to target a specific audience and communicate the message to the right people effectively. The XML signature, for instance, it wasn’t clear whether it was the Software Developer who needs to improve their methodology/practices or whether it was the web platform providers as both party seem to have the ability to address this problem.

Some of the studies reviewed (section 2.3.1, page 8) also seem to lack sound statistical basis, while it is true that cloud computing is an emerging paradigm which is built by various technologies, most of which less than 5 years ago (e.g. latest virtualization technologies such as hypervisor), system security is not new, and many organizations such as Verizon and Trustwave, among others, maintain vast amount of security related data which the public could access. For example, Engr. Farhan Bashir Shaikh and Sajjad Haider, in the paper they presented to the 6th International Conference on Internet Technology and Secured Transactions, claimed that "Cloud computing is suffering from severe security threats from the user point of view" (Shaikh and Haider, 2011) without providing substantial evidence to back their claims.

This paper is backed by the latest statistical data from various sources and focuses on the SaaS layer.

2.8.2 Future Research

The statistics show a compelling case for researchers to invest time into this multi-billion dollar industry. Cloud computing is evolving; the user base is growing, and the industry is expanding at a significant rate; as a result, innovations in cloud related technology is being introduced regularly. Cloud computing is a massive subject and surely there are many exciting areas for research that are either underexploited or unexploited. A number of related questions were raised throughout the course of this section, while the paper tries to answer most of them at the end; some of these questions deserve a more elaborate response and could be a good topic for future research.

- How do black hat hackers – hackers who hack for bad intentions - became so good, how could white hat hackers – e.g. security professionals - keep up?
- What are the implications of the PRISM program of the US government to existing data privacy laws and its effect to cloud computing adoption?
- Is there any other government in Europe running similar program -PRISM Program- ?
- Who has access to the data that were gathered through the PRISM program, who supervises the database?

3. Methodology and Fieldwork

3.1 Introduction

The answer to the question on the security of cloud based services depends on whom you ask. Understandably, the response coming from the cloud service providers is positive and assuring, while response from independent sources could be negative or positive depending on their actual experience. Hence, it is necessary to utilize several approaches to ensure a balance and reliable findings. This section describes the various research philosophies, approaches and strategies employed in the research. The relevance of the survey design, ethics compliance and participant's demographics are also explained.

3.2 Research Philosophy

It is in the best interest of cloud service providers to maintain and advance the public's trust on cyberspace, online services in particular; like the occurrence of a security related incident, a research paper that assails the trustworthiness of a cloud based service could negatively impact public trust on such service, which is bad perhaps not just for a particular provider, but for the entire industry. One of the challenges of writing about an important industry is that, when the findings go against what some group of observers wishes to hear, this group would try to resist and dismiss the findings, even worst some might accuse the author/s of untoward biases. In order to assure the integrity and accuracy of the findings, various research philosophies were applied in this study.

In order to understand the current state of cloud computing adoption, it is vital to get inputs of as many enterprise users as possible. Presumably, all things being equal, when it comes to understanding what the majority thinks about cloud computing, there is no other philosophy better than positivist. In a democratic world, majority rules, and perhaps if this would be the basis of the findings, observers will find the result difficult to assail.

Regarding the question on significant technical security issues, the views and opinions of the majority are not necessarily supreme; unless all of the participants have equal technical experience and expertise, quantitative approach may not be the best approach in this scenario. In order to understand the security issues of cloud computing better, expert's opinions were gathered. The opinions of the experts are backed by actual test results, source code analysis, website traffic monitoring and observations and other sophisticated technical approaches.

In order to improve the partiality and reliability of the result, the pragmatist's view was adopted in the study. The positivist philosophy was employed to answer straightforward questions, while challenging questions were left for the experts to interpret and deal with.

3.3 Research Approach

The research approach is apparently driven by the research question and/or objective. While the deductive approach was employed in framing the structure of the study, the research question dictates that the overall approach is inductive.

The study started with some general assumptions which were employed in the initial structure of the research activities. An exploratory study was conducted to validate and polish the assumptions, and as the research progresses, some of the assumptions were either refined or discarded as appropriate. After the study has been properly structured and focus achieved, the research activity continued on a descriptive mode; a series of related cloud security events were profiled. Finally all significant data that were independently gathered from various sources were evaluated, tabulated and analyzed. The result of the analysis done on the data then became the basis of the conclusion and recommendations.

3.4 Research Strategies

The primary objective of the study is to find out the significant technical security issues that could impede cloud adoption, SaaS based solutions in particular. This suggests that a significant part of the research is explorative in nature. The approach that was initially considered was the case study; the activities that were planned were (i) observe the security processes of the participant including physical, environmental and operational; and (ii) interview people who are involved in running the company's SaaS operation. A cloud company offering SaaS solution was approached, although the company agreed to offer some assistance, they declined to be the subject of the case study and to provide actual security data.

Both the quantitative and qualitative data used in the research were eventually gathered from various reports of independent security firms, government reports and other reliable sources. The data that were gathered are far more comprehensive as the content of reports used are based on multi modal case study involving many companies from different geographical locations. For example, the Verizon's 2013 Data Breach Investigations Report is based on the data collected from 19 contributors from around the world including the Irish Reporting

FIGURE 3.1 – DBIR Contributors

Source: Verizon's 2013 Data Breach Investigation Report

and Information Security Service (IRISS-CERT) and Verizon itself; Figure 3.1 shows the complete list of DBIR's partners. Aside from the Verizon's report, there are 8 other security and cloud computing reports/surveys used in this research; these surveys/reports are either based on actual website attack monitoring tool, source code analysis and security assessment, multi modal case study, surveys and other sophisticated and highly reliable techniques such as Symantec's Global Intelligence Network which covers more than 157 countries. Section 3.5 (page 29) provides more information about the various reports that were employed in this study.

Structured Interview is the other approach that was considered, however, since the topic is sensitive; even if assurance of total confidentiality is given, the legislation on data privacy as well as the client confidentiality prevents participant from sharing actual data. One of the Senior Managers who were approached for a possible interview on the topic, said that it is not possible to talk about cyber-attacks and data security statistics, the advised was to use various security reports instead, which are more reliable as they are based on multi modal studies covering multiple industries in various countries and the sampling population is much larger.

Presumably, due to security issues, cloud companies won't easily consent outsiders to observe their operations and would not provide actual security related data. While these companies regularly release white papers on security, they do not publicly disclose data on security breach incidents and related information. Thus, the final research strategy is multi-modal case study using secondary data published by various government and private security organizations.

3.5 Data Type and Sources

The study is largely based on quantitative data gathered from various sources. The quantitative data is also supported by qualitative data such as the outcome of technical analysis, inputs from various lectures and related materials provided by international higher institution such as Harvard University, Princeton, MIT, Purdue, Berkeley, Cambridge, among others.

3.5.1 2013 Data Breach Investigation Report

This is a global study conducted by the Verizon with the cooperation of various government and private security organizations such as the; Irish Reporting and Information Security Service, security (IRISS), the U.S. Secret Service (USSS) among others, Figure 3.1 shows the complete list. The data are based on first-hand evidence collected during paid external forensic investigations and related operations conducted by Verizon from 2004 through 2012.

Participants
19 Global Organizations studying and combatting data breaches in the world.
1. Australian Federal Police (AFP)
2. CERT Insider Threat Center at the Carnegie Mellon University Software Engineering Institute (CERT) (U.S.)
3. Consortium for Cybersecurity Action (U.S.)
4. Danish Ministry of Defence, Center for Cybersecurity
5. Danish National Police, NITES (National IT Investigation Section)
6. Deloitte (U.S.)
7. Dutch Police: National High Tech Crime Unit (NHTCU)
8. Electricity Sector Information Sharing and Analysis Center (ES-ISAC) (U.S.)
9. European Cyber Crime Center (EC3)
10. G-C Partners, LLC (U.S.)
11. Guardia Civil (Cybercrime Central Unit) (Spain)
12. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
13. Irish Reporting and Information Security Service (IRISS-CERT)
14. Malaysia Computer Emergency Response Team (MyCERT), CyberSecurity Malaysia
15. National Cybersecurity and Communications Integration Center (NCCIC) (U.S.)
16. ThreatSim (U.S.)
17. U.S.Computer Emergency Readiness Team (US-CERT)
18. U.S.Secret Service (USSS)
19. Verizon Trust Team

Sampling
47,000+ Reported Incidents 621 confirmed data breaches 44 Million Over the entire nine-year range of this study, that tally now exceeds 2500 data disclosures and 1.1 billion compromised records.

3.5.2 Website Security Statistics Report – May 2013

This report is provided by WhiteHat Security, founded in 2001 and headquartered in Santa Clara California; the company provides end-to-end solutions for Web security. WhiteHat Security has been publishing its Website Security Statistics Report Since 2006. The report is based on actual vulnerability assessment of thousands of websites across hundreds of leading organizations.

Participants
76 Organizations from the following industry 1. Banking 2. Financial Services 3. Healthcare 4. Retail Technology Industry

Sampling
Hundred Terabytes of data comprising vulnerability assessment results from tens of thousands of website across hundreds of the most well-known organizations. WhiteHat Sentinel, the company's flagship product line, currently manages more than 15,000 websites – including sites in the most regulated industries, such as top e-commerce, financial services and healthcare companies.

3.5.3 Trustwave's Global Security Report – 2013 Report

Trustwave is a leading provider of on-demand data security and payment card industry compliance management solutions to businesses and organizations throughout the world. The 2013 global security report is based on more than 450 data breach investigations in 19 countries. The goal of the report is to discover and report the top vulnerabilities and threats that have the most potential to negatively impact organizations.

Participants
5 Law Enforcement Agencies 1. US Secret Service 2. Serious Organized Crime Agency (SOCA) 3. Universidad Nacional Autonoma De Mexico CERT (UNAM-CERT) 4. New South Wales (NSW) Police Force Cybercrime Squad 5. Technology Industry

Sampling
450 Incident Response Investigation Five Million Malicious websites Nine Million Web Application 2500 Penetration Test performed against more than one million devices or websites Two Million Network and Application Vulnerability scans. 400 Web-based data breaches publicly disclosed in 2012 20 Billion emails collected and analyzed from 2007 to 2012

3.5.4 Veracodes' State of Software Security Report – April 2013

Veracode helps commercial enterprises and government agencies address the serious threat posed by hackers who are targeting software vulnerabilities to gain access to critical data. This report is based on the actual application security assessments conducted to identify vulnerabilities and validate remediation. The report examines data collected over an 18 month period from January 2011 through 2012 from 22; 430 application builds uploaded and assessed by Veracode's platform.

Participants
2000 Global Brands in 80 Countries

Sampling
Data collected over an 18 month period from January 2011 through June 2012 from 22,430 application builds uploaded and assessed by Veracode's platform. 22,430 application builds uploaded to Veracode's server for security assessment. 5 Web Programming languages/Platform 3 Mobile Platforms (Android, iOS, Java ME)

3.5.5 Imperva's Web Application Attack Report – July 2012

Imperva provides business security solution to protect high value applications and data from theft, insider abuse, and fraud. The Imperva's report is based on observing and analyzing Internet traffic to 50 web applications during the past 6 months (June-November 2011).).

Participants
Various companies worldwide not specified for security reasons.

Sampling
50 web applications observed and analyzed during the observation time frame December 2011 to May 2012 (6 months).

3.5.6 Symantec's Internet Security Threats Report – April 2013

Symantec protects the world's information and is a global leader in security, backup, and availability solutions. This report is based on the data gathered by Symantec's Global Intelligence Network; the network is consisted of about 69 million attack sensors, logs thousands of events per second and monitors over 157 countries and territories.

Participants
157 countries and territories 50 million consumers

Sampling
51,644 recorded vulnerabilities 16,687 vendors 43,391 products

3.5.7 CDW's State of The Cloud Report – 2013

CDW is a leading provider of technology solutions for business, government, education, and healthcare. This report is based on the views of 1,242 IT professionals who responded the survey. The survey explores what drives the shift to the cloud, what types of applications businesses are taking to the cloud and what benefits (beyond cost savings) they are achieving.

Participants
1,242 professionals from 7 Industries and various level of responsibilities 1. Small business 2. (20-99 employees) Medium business 3. (100-499 employees) Large business 4. (500+ employees) Federal government 5. State & local government 6. Healthcare 7. Higher education 8. K-12 public school districts Various Levels 1. Chief/Deputy CIO 2. Chief/Deputy CTO 3. IT Director/Manager 4. IT Supervisor/Specialist 5. IT Systems Engineer

Sampling
12% Chief/Deputy CIO 7% Chief/Deputy CTO 45% IT Director/Manager 24% IT Supervisor/Specialist 12% IT Systems Engineer 1. Small business - 155 2. (20-99 employees) Medium business - 155 3. (100-499 employees) Large business - 157 4. (500+ employees) Federal government - 155 5. State & local government - 155 6. Healthcare - 156 7. Higher education - 157 8. K-12 public school districts - 152 Total = 1242

3.5.8 Information Week Reports' State of Cloud Computing Survey – May 2013

InformationWeek is an authoritative source of information for the global IT community; operating for more than 30 years, the services they provide has helped millions of business technology executives worldwide. This survey is based on the 446 business technology professionals across various industries.

Participants
446 Business Technology Professionals at organizations with 50 or more employees from the following Industries 1. Construction/Engineering 2. Consulting and business services 3. Consumer goods 4. Education 5. Electronics 6. Financial Services 7. Government 8. Healthcare/Medical 9. Insurance/HMOs 10. IT Vendords 11. Manufacturing/Industrial, noncomputer 12. Media/entertainment 13. Retail/e-commerce 14. Telecomunicaitons/ISPs 15. Utilities Other

Sampling	
1. Executive IT Mangement (C-level.VP)	- 7%
2. IT director/manager	- 30%
3. Consultant	- 6%
4. Line-of-business management	- 3%
5. Non-IT executive management	- 4%
6. IT/IS Staff	- 41%
7. Other	- 9%
Total = 446	

3.5.9 2012 Cost of Cyber Crime Study: - Ponemon Institute

Ponemon Institute conducts independent research on privacy, data protection and information security policy. This is a benchmark study of US Companies independently conducted by Ponemon Institute Michigan USA. The study is based on 56 organizations in various sectors located in the U.S., the United Kingdom, Germany, Australia and Japan.

Participants
56 Organizations in various industry sectors located in the US, the UK, Germany, Australia and Japan

Sampling
100% Large organizations with more than 1000 enterprise seats.

3.6 Lessons Learned

Data security is a serious topic; cloud service providers – understandably, being a data keeper -, are sensitive about this issue. This sensitivity is manifested in how cloud companies react on data breach reports. While companies such as Sony, Yahoo, LinkedIn, Facebook, Apple and many other who were recently fell victims of cyber-attacks, confirmed the negative reports; they always stress that the data remain safe/uncompromised, or only limited data have been compromised, and that they are taking necessary steps to improve data security. The reaction is understandably valid as data security is inherently important part of their business; any loss of trust could significantly impact their user base.

The possibility that these companies will allow outsiders to do on-site visits and/or to tap in to their database to observe and analyze how the company is doing in terms of securing user's data is very slim - if it is possible at all in the first place-. In order to gather security related data from a cloud provider, the researcher needs more than just a guarantee of total confidentiality; perhaps, a significant tie with the organization and/or being a member of a reputable research institution could give the researcher a better opportunity to get these companies to participate.

The two most valuable lessons I learned from conducting this research are: (i). data security is a serious topic and data collection could be a challenge and (ii) data from secondary sources - provided by reputable organizations – could be more reliable than data collected by individual researchers, graduate researchers in particular, because organizational reports or data sources are in general, based on a more rigid study – multiple methodologies, data were taken from a variety of reliable sources, participants and data samples are much bigger, data are highly triangulated, the study is undertaken by multiple professional researchers-.

3.7 Limitation of the Methodology

Although all the reports and other data sources used in this study were carefully analyzed and evaluated before they were considered – methodology used by the researchers, biases of researchers, accuracy of analysis and data tabulation, technical skills and resources available to the organizations, and the reliability of the organizations in general -, the fact remains that the data are based on secondary sources. While the data gathered from secondary sources could be as relevant as the data that primary sources provide, the accuracy of the report could still be improved by undertaking similar surveys and studies of the same scale, as done by publishers/researchers of the secondary sources; however, doing

so is impractical given the amount of time and resources required to achieve the same level of rigidness. For example, source code analysis requires expertise on secured programming aside from time required to do the actual analysis; web traffic monitoring requires software tools and specific skills on the part of the researchers. Likewise, getting appropriate and reliable research participants and data sample such as IT executives, multinational companies, among others, to participate in simple surveys could likewise be challenging for graduate researchers.

4. Findings and Analysis

4.1 Introduction

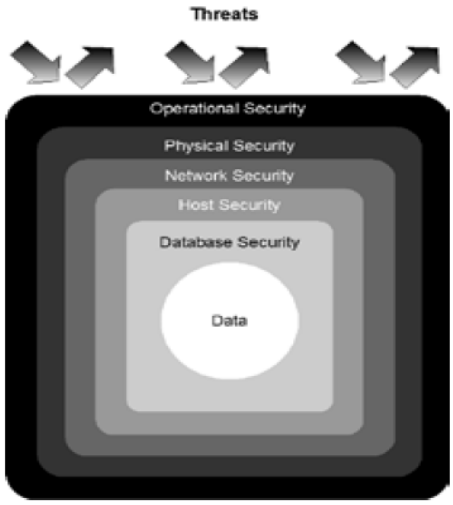


FIGURE 4.1 - Force.com security layers of defense

Source taken from SalesForce Whitepaper (2010).

Cloud computing is disruptive; its popularity among the business community had created a sense of urgency among today's global IT players to focus their attention into this promising industry. DELL, Apple, Google, Microsoft, Oracle, SalesForce, Amazon are only some of the major IT players that have targeted this emerging market. While the demand for cloud based services, undeniably, created a significant market size, some experts believe that it is still smaller than expected. Surveys (InformationWeek, 2013) (CDW, 2013) show that while many companies have embraced the cloud, security remains a significant barrier to cloud adoption.

This section presents the research finding which includes the following: what major cloud companies are doing to ensure data security and privacy, the various threats to SaaS platforms, the different levels of technical vulnerabilities, the current state of cyberspace security and the significant technical security issues of cloud based applications. The methodology used in data analysis and interpretations are also discussed in this section.

4.2 Data Security and Privacy in the Cloud

A cloud based software solution also known as Software as a Service (SaaS), processes and stores sensitive personal and financial data in a remote server. Hence, the security and reliability of the platform is highly critical. Cloud providers acknowledge that data security is a significant concern for the users, so they consistently assure users that their respective SaaS platform is secure and reliable. In order demonstrate commitment to data security and gain user's trust; SaaS providers such as SalesForce, Google and Amazon among others regularly release security compliance white papers (Table 4.1) explaining the different security layers and procedures they have in place; they also consistently seek certifications,

accreditations and third party attestations to boost user's trust. Figure 4.1 shows the various layers of defense that SalesForce employs to counter threats to data security; other major cloud providers such as Amazon and Google employ similar defense structure.

TABLE 4.1 - Major Cloud Providers Security White Papers

Company	Security White Paper	Location/URL
Amazon	Amazon Web Services: Overview of Security Processes.	http://awsmedia.s3.amazonaws.com/pdf/AWS_Security_Whitepaper.pdf
Google	Security Whitepaper: Google Apps Messaging and Collaboration Products.	http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/a/help/intl/en-GB/admins/pdf/ds_gsa_apps_whitepaper_0207.pdf
SalesForce	Secure, private, and trustworthy: enterprise cloud computing with Force.com.	http://www.salesforce.com/assets/pdf/misc/WP_Forcedotcom-Security.pdf
Microsoft	How Microsoft Addresses the four top cloud computing issues.	http://www.microsoft.com/en-ie/cloud/tools-resources/whitepaper.aspx?resourceId=Cloud_Positioning

TABLE 4.2 - Various Cloud Computing Relevant Security standards

Standard
SOC1/SSAE 16/ ISAE 3402
SOC 2
FISMA
DIACAP
FedRAMP
PCI DSS Level 1
ISO 27001
ITAR
FIPS 140-2

It is indisputable that SaaS providers, the major ones in particular, are doing enough to assure data security; however, the fact remains that while they align their security practices to various IT security standards such as listed in Table 4.2, cloud based services could still be seen as vulnerable as hackers continuously operate and make headlines. What is more alarming is the fact that Government could also be a source of threat. Edward Snowden, a NASA contractor who revealed how the US government spied on its people via a project called PRISM, delivered a clear message: data stored in the cloud can be reviewed and that promise of data privacy cannot be trusted.

Perhaps another problem is enforcement of regulations; Shahed Latif, Principal KPMG in the US, argued that while primary cloud computing markets such as the US, the UK and China slowly standardizing aspects of cloud computing its enforcement is weak even after the regulations are being promulgated (KPGM, 2013).

Arguably, lack of standards particularly in security could result to a less secure cloud platform.

4.3 The threats to SaaS Platform security

Surveys, security experts and scholars, consistently cite data security and privacy as the most significant challenge to cloud adoption (section 2.3.1, page 8). This was confirmed by the global survey done by KPMG (2013); the study shows that while the respondents "are starting to fully appreciate the transformative value that cloud can bring to the enterprise" (KPGM, 2013) security remains significant concerns for IT and business executives. Furthermore, the 2013 State of Cloud Computing report issued by the Information Week shows the 51% of their 446 respondents are being held back from adopting cloud due to cloud related security fears, 48% due to data security and privacy of companies' proprietary data and 40% for fear of unauthorized access to the companies' customer's information (see Figure 4.2).

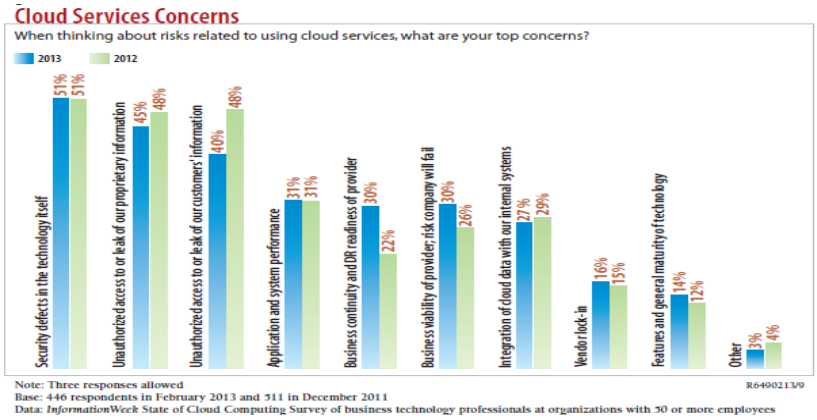


FIGURE 4.2 - Cloud Service Concerns
Source adapted from Information Week (2013). *State of Cloud Computing*

This section presents the various layers of platform security that the major cloud providers use to resist various types of security threats.

4.3.1 Operational Security Layer

While companies now employ various security checks and control to prevent data security breach, insiders remain a significant threat to data security. Based on the 2013 Data Breach Investigations Report by Verizon, 14% of security breaches were caused by insiders. Figure 4.3 shows the perpetrators of the recorded breaches.

The access privilege and operations that an employee can perform inside the facility determines the security threat that he/she poses to data security. Shane Robinsons of SANS argued that companies who employ the corporate espionage use both ethical and unethical means to obtain confidential information (SANS Institute, 2007). He suggested that companies hire people - either employees of a rival company or a 3rd party company-, to act as spies. Corporate spies usually employ both technical and non-technical method to gain access to restricted resources, Table 4.3 shows the various techniques employed in corporate espionage.

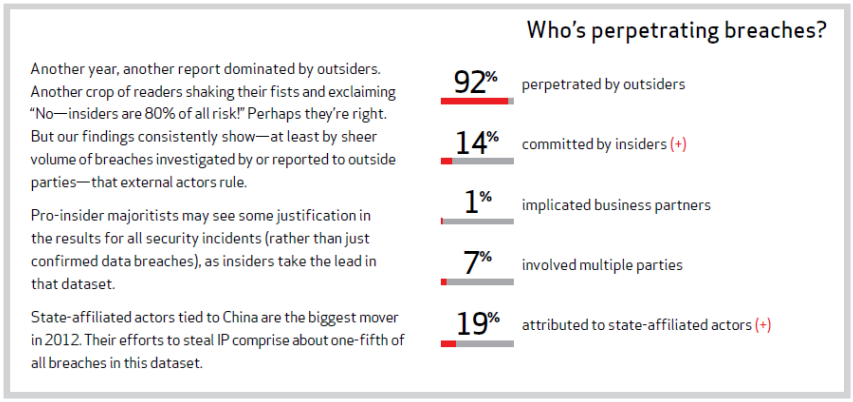


FIGURE 4.3 - Who's behind data breaches?

Source taken from Verizon Enterprise (2013). Data Breach Investigation Report

TABLE 4.3 - Techniques employed in corporate

Source adapted from SANS Institute (2007). *Corporate Espionage 201*

Techniques	Description
It's All There in Black and White	Spies target documents, containing sensitive data, which were sent to a network printer for printing.
Oldie But Goodie	Corporate spies use keylogger to spy on a specific employee, the keylogger records all the keystrokes of the users and send it to a designated email address.
More Power to Ya	Attackers are able could gain access to a corporate network by using Ethernet over Power (EoP). This is done by using an EoP device that could turn the building's electrical wiring into a 56-bit encrypted network, the attackers are then able to connect to the network undetected.
A Tale of Two APs	The spy creates an illegitimate access point (AP) to lure his victim to connect; once the target connects the spy is now able to perform a man in the middle attack which enable him/her to capture sensitive data that passes through the fake AP.
USB	With decreasing size, increasing speed (USB 3.0), and increasing storage capacity, spies are able to copy massive amount of corporate data very quickly and seamlessly.
A Host with Dual Personalities	Bootable OS such as Linux allows attackers to bypass domain security policies, meaning by using a bootable OS, users are able to completely takeover the PC as administrator with all the ports open.

4.3.2 Physical and Environment Security

The September 11 terrorist attack on the World Trade Center had underscored the importance of physical and environmental security. Businesses had learned the hard way that the physical locations of the data –both the active and backup data storage - are also vulnerable and therefore should also be protected. Assuming that reliable technologies and industry standard devices and best practices are used (e.g. custom designed electronic card access control system, alarm systems, interior and exterior cameras, security guards), perhaps the biggest threat to this layer is poor disaster recovery planning. For example, several businesses located in or around the World Trade Center had their back-up centers just a few blocks away which, unfortunately, were also crippled by the attack. Francis Monaco, in the article he wrote for Educause Quarterly, stressed the need to choose a disaster recovery provider whose data center is away from the companies' site (Monaco, 2001).

While the major cloud players do not seem to have problems in this area, the small and medium ones might find it costly and unable to implement a robust disaster recovery plan and/or the same level of physical and environmental security.

4.3.3 Network Security

Perhaps the biggest problem on network security is still the Denial-of-service Attack (DoS), as observed several times, this attack can shut down an entire website - SaaS platform in particular- by sending massive volume of traffic to the target server; Cisco Systems argued that no company is immune from this and similar attacks (Cisco Systems, 2006). The challenge here is how to isolate the malicious request from the legitimate ones when both requests look exactly the same. While the technique of load balancing could prevent the immediate crash of the system, it has a tipping point and once the maximum load is reached, it would eventually cause a server crash just like what happened to MasterCard, PayPal and many other companies during the height of the Wikileaks issue in 2010.

Cloud providers such as SalesForce, Google, Microsoft and Amazon undeniably, have adequately secured networks; the white papers that that these and other major cloud players regularly release are reassuring. While all the security process, accreditations and credentials they have are impressive, none of these companies guarantees total network security or DDoS attack free network. Apparently, at the moment, the competition is only about who provides more security rather than absolute security.

4.3.4 Host Security

The term host refers to the server that runs the web application. In an enterprise environment, server is a machine with a server grade Operating System (OS) such as Windows Server or UNIX server. It is a major component of a SaaS platform as it host's the SaaS solution. If networking technology is not mature enough to prevent various attacks such as DDoS, the OS technology, after more than 60 years in development undergoing various improvements particularly in the security area, is seen to be a matured technology in terms of security.

Conceivably all the tools that a system administrator needs to manage the security of the host are now available. For example, Microsoft's domain controller technology, particularly Active Directory (AD) has significantly improved computer security, those who understand this particular technology will likely agree, the fact that businesses are willing to pay a fortune to have this technology deployed to their production environment is a proof.

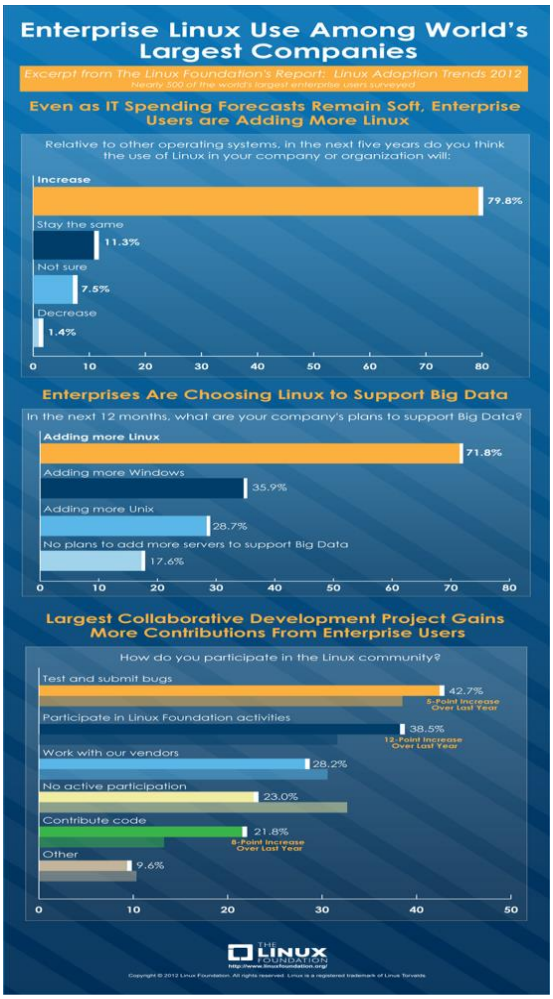


FIGURE 4.4 – Linux Adoption

Source taken from McPherson, A. (2012). *Linux Adoption Trends 2012: A Closer Look.*

It can be argued that local servers assuming that proper standard security policies were applied are safe. While there are still threats emanating from the employees who have access to the server, companies now have enough experienced to address such problem, they employ a combination of access control and operational policies. For instance, Salesforce does a thorough background check on employee or contractor before granting them access to the facility. The staffs' access to resources is subsequently controlled by employing a combination of technology and operational approach in data security such as utilizing secure workstation to prevent cut/paste, public IM and data copying; tight segregation of duties (least privilege); and private networks (SalesForce, 2010).

Perhaps the only remaining major issue in this area is the OS's code transparency. Leading OS providers such as Microsoft do not distribute the source code that allows the customers' to review and evaluate the OS's security. The efforts of emerging OS providers such as Red Hat Linux to capitalize on OS transparency issue seem to be a success, as Linux Adoption has been accelerating over the years. The most recent report conducted by Linux foundation in cooperation with Yeoman Technology Group entitled Linux Adoption Trends 2012: A Survey of Enterprise End Users shows that Linux is the top choice among world's largest companies (Figure 4.4).

4.3.5 Database Security

The final layer that secures data is the database layer. It plays a significant role in platform security as it ultimately determines the success of an attack. Just like all the previous security layers, the human element of the platform is a major threat to data security, but assuming that this threat has been taken care of at the operational security layer, perhaps the biggest source of threat against this layer could come from the web application, as well as its users. The data is only exposed to the user by the database layer via a legitimate request from the web application – after user account validation etc. -; in a well secured platform, hackers do not have direct access to the data but through the application that is exposed to the users. In order to initiate an attack, a hacker need a valid user account to gain access to the application, they can apparently do it in two ways, (i) illegally obtain credential of a valid user or (ii) legally sign up for the service. Once a hacker has obtained a valid credential either ways, he could start learning his way to the system, testing the vulnerability of the application with the goal of exploiting it to gain access to the restricted data.

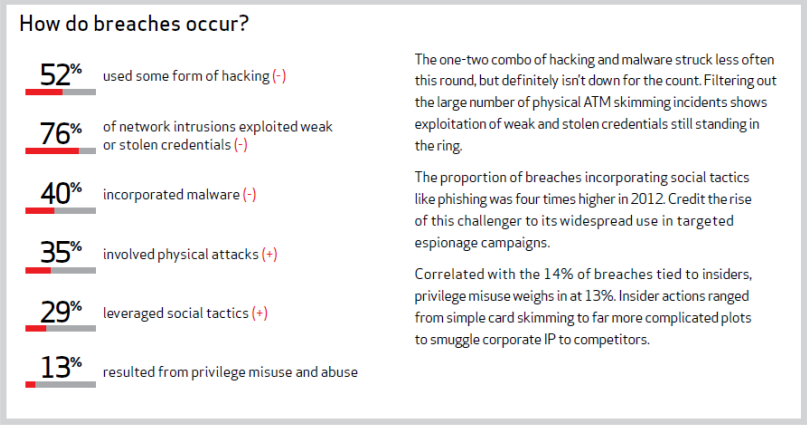


FIGURE 4.5 – How do breaches occur?

Source taken from Verizon Enterprise (2013). Data Breach Investigation Report

The 2013 Data Breach Investigations Report (DBIR), shows that 92% (Figure 4.3) of the 47,000+ data breaches were committed by external agents, of this 43,220 cases, 52%

(Figure 4.5) was due to hacking, which means hacking accounts for approximately 22,000+ data breach incidents. Apparently an unsecured web application could expose the data to unauthorized users and renders all other layers invalid.

4.4 Application Layer Vulnerability

The risks associated with the applications deployed to the cloud or enterprise servers have been gaining attention in the recent days. The most recent successful attacks against many multinational companies were reportedly due to the vulnerabilities of web applications and/or its software component/s. For example, Apple and Facebook stated that the successful attack to their system was due Java Software they use. Veracode, on its 2011 State of Software Security Report, claimed that Cross-site Scripting and SQL injection are the most frequently exploited vulnerabilities.

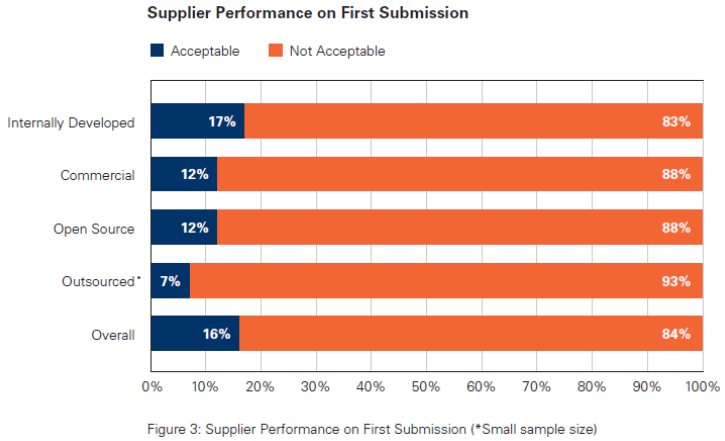


Figure 3: Supplier Performance on First Submission (*Small sample size)

FIGURE 4.6 - Application Security Acceptability

Source taken from Veracode (2011). Volume 4 State of Software Security Report

Figure 4.6 shows how application suppliers perform in terms of Application Security as rated by Veracode (2011).

Application Type and Programming Language by Supplier Type

	C/C++	ColdFusion	Java	.NET	PHP	Web	Non-Web
Internally Developed	4%	1%	60%	28%	6%	77%	23%
Commercial	15%	4%	48%	27%	7%	67%	33%
Open Source	21%	0%	55%	9%	13.3%	48%	53%
Outsourced*	2%	1%	60%	29%	7%	94%	6%

Table 1: Application Type and Programming Language by Supplier Type (*Small sample size)

FIGURE 4.7 - Application Type and Programming Language

Source taken from Veracode (2011). Volume 4 State of Software Security Report

Java appears to be the language of choice for web applications (Figure 4.7), and hacking is the leading threat action (Figure 4.8). As application security acceptability level is less than 20% which is alarming, Java Web Developers urgently need to know and understand the commonly exploited vulnerabilities to be able to address them. The following sections explain the characteristic and working of the most prevalent vulnerabilities.

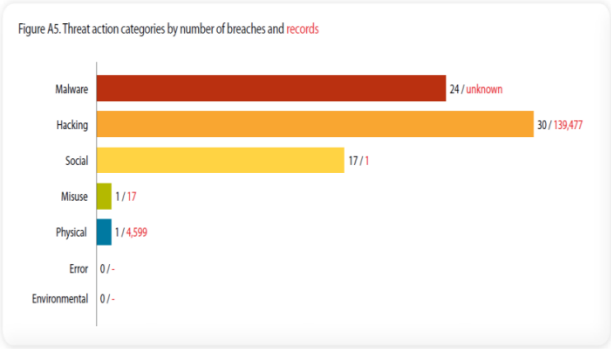


FIGURE 4.8 – Threat action categories by number of breaches and records.

Source taken from Verizon Enterprise (2011). Data Breach Investigation Report

4.4.1 Cross-site scripting (XSS)

XSS is a hacking technique that takes advantage of the website's trustworthiness; what it does is it injects malicious code into a legitimate website, which unsuspecting users execute resulting to a potential breach of privacy (Leason et. al, 2012). Some of the goals of the XSS include session hijacking or drive-by download of malware. While XSS code only executes within the confines of the browser, it can create a further attack entry points by tricking the victim to download malware. This technique could potentially allow the attacker to steal browsing session and impersonate the victim, track web history and information entered into forms. There are cases where an XSS attack could also track the victim's physical location and ultimately turn a computer into a zombie computer that could be controlled by the attacker.

The paper "Automatic Creation of SQL Injection and Cross-Site Scripting Attacks", presented at the 31st International Conference on Software Engineering in Vancouver claimed that both Cross-site scripting (XSS) and SQL Injection (SQLi) are widespread forms of attack (Kiezun et al., 2008). Figure 4.8 shows that hacking tops the list of threat actions which suggests that the attacks were done remotely; at the application level SQLi, XSS, cross site request forgery appears to be the most prevalent types of hacking (Verizon Enterprise, 2011).

The Veracode's 2011 State of Software Security Report shows that indeed application providers do not do well in terms of XSS attack; Figure 4.9 suggests that internally developed, commercial and outsourced applications have serious XSS vulnerabilities.

Vulnerability Distribution by Supplier

Internally Developed		Commercial		Open Source		Outsourced*	
Cross-site Scripting (XSS)	58%	Cross-site Scripting (XSS)	44%	Cross-site Scripting (XSS)	41%	CRLF Injection	47%
CRLF Injection	12%	Information Leakage	11%	Directory Traversal	13%	Cross-site Scripting (XSS)	28%
Information Leakage	10%	CRLF Injection	8%	Information Leakage	13%	Information Leakage	6%
SQL Injection	4%	Directory Traversal	6%	CRLF Injection	11%	Encapsulation	6%
Cryptographic Issues	3%	Error Handling	5%	Cryptographic Issues	8%	Cryptographic Issues	5%
Encapsulation	3%	Cryptographic Issues	5%	SQL Injection	3%	Credentials Mgmt	3%
Directory Traversal	3%	Buffer Mgmt Errors	4%	Error Handling	2%	Directory Traversal	2%
Insufficient Input Validation	1%	Buffer Overflow	3%	Time and State	2%	API Abuse	1%
Time and State	1%	Potential Backdoor	3%	API Abuse	2%	Time and State	1%
Race Conditions	1%	SQL Injection	3%	Insufficient Input Validation	1%	Insufficient Input Validation	1%

FIGURE 4.9 - Vulnerability Distribution by Supplier

Source taken from Veracode (2011). Volume 4 State of Software Security Report

4.4.2 SQL Injection

Professor's Avi Kak of Purdue University described SQL Injection as an application vulnerability that allows hackers to run unauthorized operations on the database (Kak, 2013). It is done by providing additional SQL statements on unsecured input fields of a webpage. These additional SQL statements then then became part of the poorly coded SQL statements in server side code. As the original statement executes so as the ones that were added by the attacker; the outcome is the data that is returned to the user includes the targeted data.

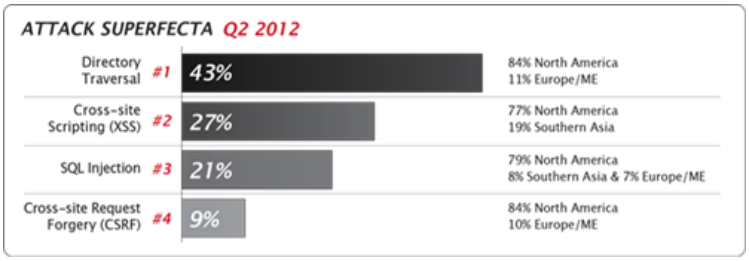


FIGURE 4.10 - Superfecta Attack Q2 2012

Source taken from Firehost (2012). Web Application Attack Report

Both the Verizon and Veracode Reports consider SQL injection as widespread; Firehost, a provider of secured cloud computing platform, classified SQL Injection as a Superfecta attack, which in FireHost's definition the most malicious and dangerous attack on web application. Figures 4.10 to 4.11 show that SQL injection attack rose to 21% in Q2 of 2012, an 11% rise from Q1 2012.

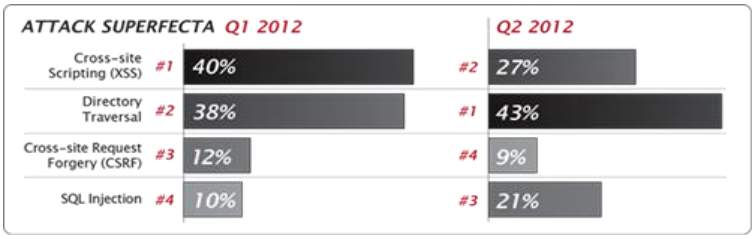


FIGURE 4.11 - Superfecta Attack Q1 2012

Source taken from Firehost (2012). Web Application Attack Report

4.4.3 Directory Traversal

Mike Danseglio a Certified Information Systems Security Professional (CISSP) and an operation manager of the Xbox LIVE operations team, described Directory Traversal (DT) as an attack against a Webserver that allows the hacker to view restricted files on the server. He claims that it is a great exploit as it allows hackers to gain access to passwords and other confidential information on files stored in the server (Danseglio, 2002). This vulnerability is both present on Linux and Windows platforms.

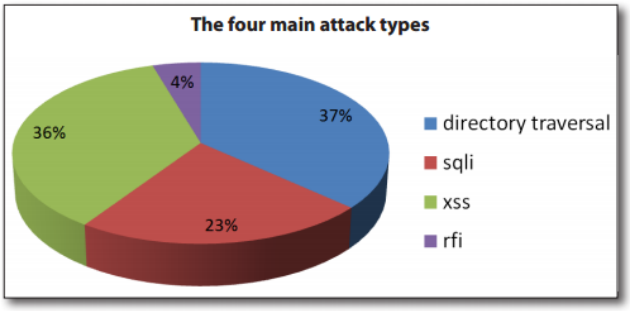


FIGURE 4.12 - The Four Main Attack Types

Source taken from Imperva (2011). State of Software Security Report

The 2011 Web Application Attack Report by Imperva, listed directory traversal as a dominant attack type, Figure 4.12 shows the top four most dominant attacks; the data was based on the 10 million suspicious event monitored by Imperva's Application Defense Center. The data suggest that the majority of the attacks came from major cloud computing market such as the US, China and the European Union; Table 4.4 presents the top sources of attacks.

TABLE 4.4 - Sources of Attacks – Imperva

RFI		SQLi		DT	
Country	**Attacks**	**Country**	**Attacks**	**Country**	**Attacks**
USA	20918	USA	91606	USA	189474
United Kingdom	1897	China	47800	Sweden	13535
Netherlands	1879	Sweden	8789	France	9417
France	1253	Indonesia	3604	Netherlands	8320
Republic of Korea	1070	United Kingdom	3419	Germany	7656
Germany	1030	Netherlands	2793	United Kingdom	6692
Sweden	1012	Ukraine	2489	European Union	4159
Brazil	506	Republic of Korea	2374	Canada	3492
Russian Federation	490	Romania	2136	Republic of Korea	2838
European Union	460	Germany	1263	China	2507

Source taken from Imperva (2011). Volume 4 State of Software Security Report

4.4.4 Cross-site Request Forgery (CSRF)

Vijay Ganesh (2013), Assistant Professor Computer Security in the University of Waterloo, Ontario Canada, described CSRF as an attack against a web application where a malicious website visited by the user is used to perform an attack to a trusted website (e.g. a bank website). William Zeller and Edward Felten of Princeton University in their paper entitled "Cross-Site Request Forgeries: Exploitation and Prevention" branded CSRF as the "sleeping

giants of web vulnerabilities", because despite the serious threats that it poses, the web and security communities largely ignore it (Zeller and Felten, 2008).

The May 2013 Website Security report of White Hat, (Figure 4.13) shows that CSRF is a common vulnerability, with 26% of all the websites analyzed vulnerable to such attack.

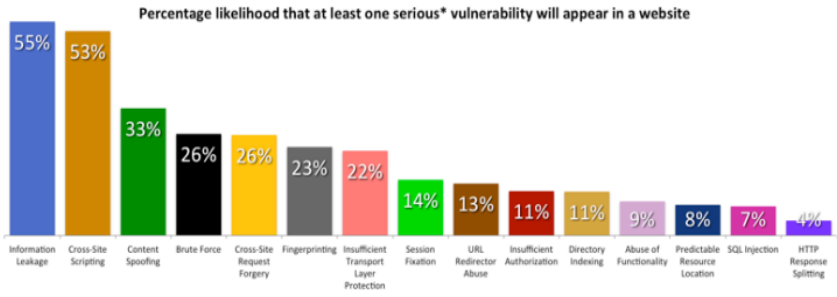


FIGURE 4.13 – Top 15 Vulnerability Classes

Source taken from WhiteHat (2013). Volume 4 State of Software Security Report

4.5 Hardware Layer Vulnerabilities

Though the hardware component of a SaaS platform also has some vulnerability, there is not a lot known that poses immediate threats to data security. Regardless which report you look at, hardware vulnerability is not an immediate concern. Perhaps what is worrying in this area is that hardware manufacturers do not take full responsibility in case the device that they distribute causes a security breach. Sergei Skorobogatov, in his technical report on Hardware Security presented to the University of Cambridge United Kingdom (Skorobogatov, 2005), claimed that some hardware manufacturers are not strict when it comes to the proper design and testing of protection mechanism of their product/s. While manufacturers claim high level security, they give no guarantee and accept no responsibility if a device is compromised.

While it is true that at present software vulnerabilities is the one needing urgent attention (Table 4.5), hardware security is apparently also important as the discovery of major hardware vulnerability could have an unimaginable repercussion to the cloud computing industry.

TABLE 4.5 - Current State of Website Security 2012

Industry	Avg Vuln Sites	Annual Avg Vulns	Remediation Rate	Avg. Time-to-Fix (Days)
All	86%	56	61%	193
Entertainment & Media	91%	12	81%	33
Financial Services	81%	50	67%	226
Retail	91%	106	54%	224
Technology	85%	18	61%	71
IT	85%	114	54%	185
Healthcare	90%	22	53%	276
Banking	81%	11	54%	107
Manufacturing	100%	27	55%	197
Social Networking	86%	20	46%	175
Telecommunications	89%	20	74%	163
Education	100%	47	58%	342
Energy	100%	59	71%	144
Insurance	78%	39	55%	274
Government	100%	8	65%	48

Source adapted from WhiteHat (2013). Volume 4 State of Software Security Report

For example, there could be a massive break down on trust on data integrity and privacy if someone discovers that a network device is stealthily sending data to a remote server. The cloud computing community, particularly SaaS providers, while addressing the software threats, also has to work with hardware manufacturers to make sure that hackers won't find hardware based backdoor to the system.

4.6 Protocol Layer Vulnerability

The majority if not all of the existing networking protocol standards are either created or endorsed by the International Standard Organization or ISO. The OSI Open Systems Interconnection (OSI) model, which is consider to be the primary networking model, for instance, was the work of the joint technical committee of the ISO and the International Standardization Sector (ITU-T). Standards development such as the OSI model is a rigid and laborious multi-stakeholder process; the process has 6 stages and involves global industry experts and stakeholders from various associations, academia, NGOs and government organizations. With ISO's very rigid process, it is high likely that a flawed or loosely defined protocol and/or model will pass the technical committees' scrutiny.

The study did not find any security issues on any of the most popular internet and related protocols that are widely used today; the various technical reports and studies examined in the preparations of this paper did not mention any problem on any specific protocol that had caused any significant technical issue.

4.7 Cyberspace Security

Dr. David Clark, a Senior Research Scientist at the Massachusetts Institute of Technology, described cyberspace as the "collection of computing devices connected by networks in which electronic information is stored and utilized, and communications takes place" (Clark, 2010). For the purposes of this study, Internet adopts the same meaning.

The Office of Science under the U.S. Department of Energy on its Report entitled "Report of the Cyber Security Research Needs for Open Science Workshop" (DOE Office of Science, 2007); argue that the threats coming from cyberspace has grown significantly to an alarming state. The report suggests that individuals, organizations and states' enhanced ability to attack US institutions and people online are worrying. The report further claims the United States' heavy reliance on web and other emerging communication and collaboration technologies made the US vulnerable to cyber attackers from around the world. The US

according to the report and this is perhaps also true for many other countries such as Ireland, rely on IT for the day to day operations of running companies, organizations and government. The Internet or the cyberspace is a public utility/space; hence, anyone including criminals, scammers and the like can easily get online and perform illicit activities. Arguably, these illegal activities in the cyberspace flourished because law enforcement is either weak or the perpetrators are simply smart and difficult to trace. At present, virtually all public cloud services are delivered over the Internet, which makes them vulnerable to attacks. While cloud providers regularly issue security assurance through white papers and other mediums, the ever growing number of reported data breaches (Verizon Enterprise, 2013), unfavorable security assessment results (Imperva, 2012), reports on successful cyber-attacks and the existence of known and unknown threats against web applications, are arguably the biggest impediments in the realization of a cloud based society.

4.8 Cloud Adoption

In 2011, the US government's CIO presented a 20 billion dollar strategy that had significantly promoted cloud computing; the strategy called for almost a quarter of the entire federal IT spending to move to the cloud (McAfee, 2011). Many private companies followed suit, pushing the global cloud market to $89 billion in 2011 (Gartner, 2011). Gartner had estimated that cloud will continue to grow at 17.7% compound annual growth rate from 2011 to 2016, the prediction is proven to be accurate as global cloud expenditures continues to grow at double digits.

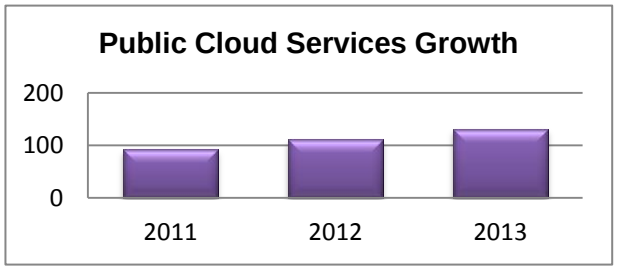


FIGURE 4.14 - Cloud Adoption Gartner from 2011-2013 in Billion

Source: Gartner

4.8.1 Cloud adoption is slowing

InformationWeek's 2013 State of Cloud Computing survey shows that while cloud adoption is still on an upward track, it is slowing. According to the report, 51% (Figure 4.15) of the 446 respondents are being held back from implementing cloud due to security concerns and the SaaS adoption is down 8 points since last year's survey. The survey was participated by business technology professionals (Figure 4.16) from companies with 50 and more employees (Figure 4.17), and whose revenue ranges from less than $6 million (7%) to $5 billion or more (14%); (Figure 4.18) more than 15 industries are represented in the survey (Figure 4.19).

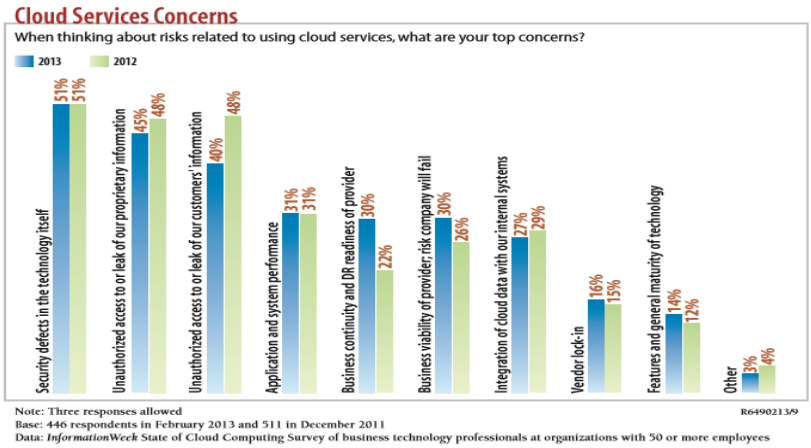


FIGURE 4.15 - Cloud Services Concerns

Source: InformationWeek 2013 State Of Cloud Computing

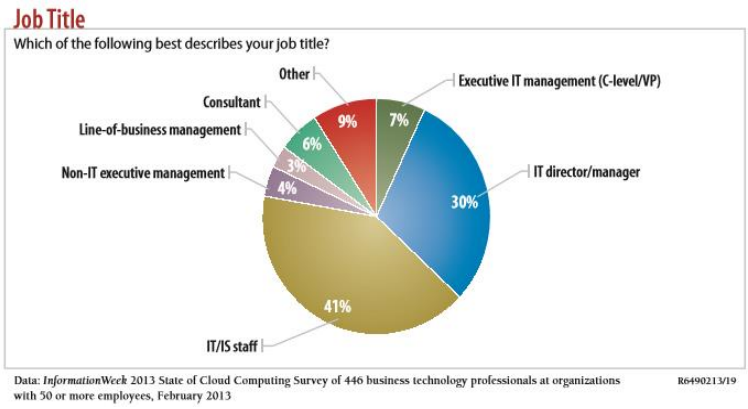


FIGURE 4.16 - Participant Demographics

Source: InformationWeek 2013 State Of Cloud Computing

Perhaps many businesses and IT strategies that rely on the media for information regarding cloud growth are under the impression that cloud adoption is massive. For instance, Garner's estimates and forecasts on cloud computing's current state and growth paints a very positive outlook; the numbers which are expressed in billions of dollars are truly stunning; however, specific surveys seem to show a less rosy picture and presumably a more accurate view of the current state of cloud computing; Figure 4.20 shows that still less than half of the 446 respondents are receiving services from a cloud provider, with one of the respondents saying "I won't trust my checkbook to the cloud, why should I trust anything else?".

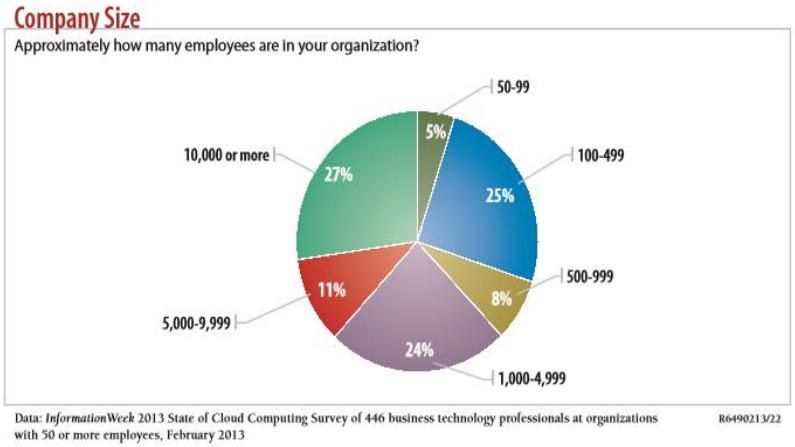


FIGURE 4.17 - Company Size by Number of Employees

Source: InformationWeek 2013 State Of Cloud Computing

FIGURE 4.18 - Company Size by Revenue

Source: InformationWeek 2013 State Of Cloud Computing

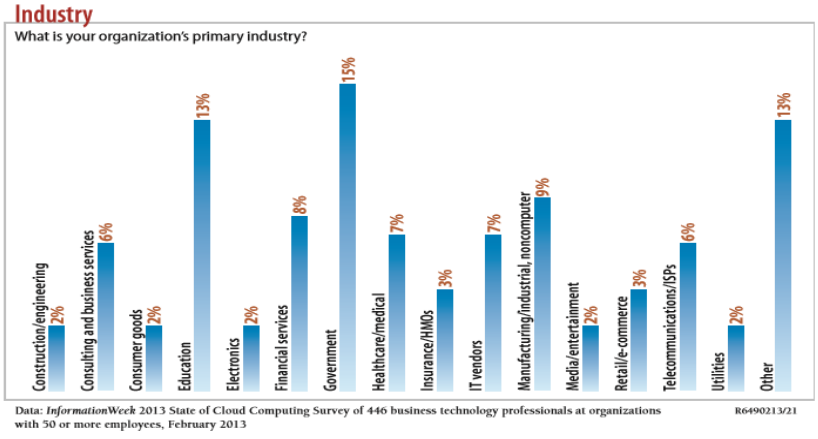
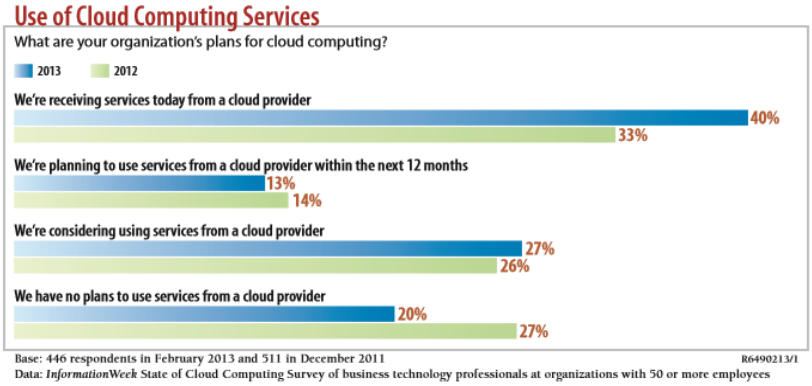


FIGURE 4.19 - Industry of the participants

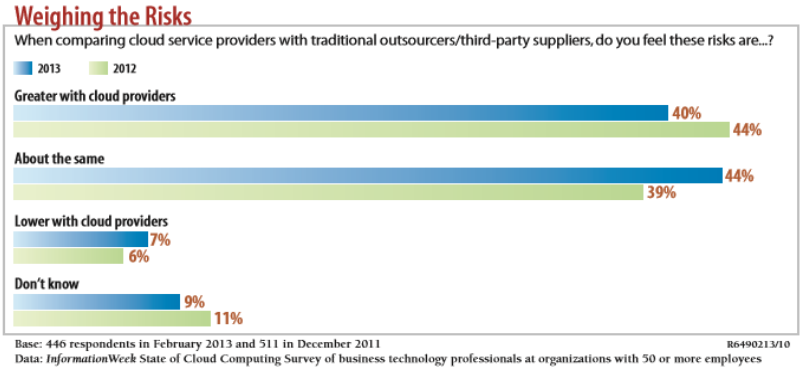
Source: InformationWeek 2013 State Of Cloud Computing



The figure suggests that cloud adoption is still on upward track.

FIGURE 4.20 - Use of cloud computing services

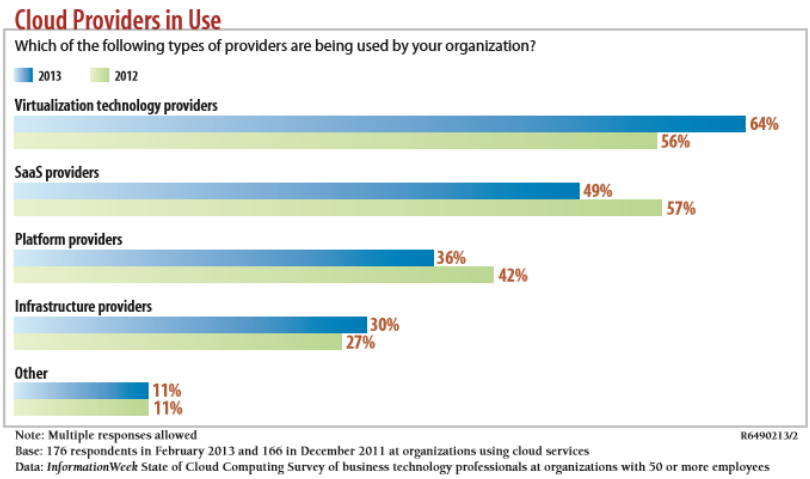
Source: InformationWeek 2013 State Of Cloud Computing



In terms of Risks, cloud service providers are not considered to be riskier than outsourcers and/or third party suppliers.

FIGURE 4.21 - Weighing the Risks

Source: InformationWeek 2013 State Of Cloud Computing



SaaS utilization went down by 8 points note that the top 3 concerns of the participants are all related to security (Figure 4.15)

FIGURE 4.22 - Cloud Services in Use by organizations

Source: InformationWeek 2013 State Of Cloud Computing

While the overall cloud adoption continues to follow an upward trend, SaaS adoption significantly went down in 2013 by 8 points. The drop on SaaS adoption does not seem to be due to trust issue with the cloud provider; 44% said that the risks dealing with cloud providers are just about the same as dealing with traditional service providers. Considering that security remains the top concerns for the respondents – Figure 4.15 top 3 concerns all related to security -, and the fact that users have no control in terms of security of a SaaS platform, security was a significant factor in this slump. Yet, the 24 month outlook is still positive, as the majority of the respondents predicted that a significant amount of IT services will still be delivered over cloud; only 5% said they hated the cloud (Figure 4.23).

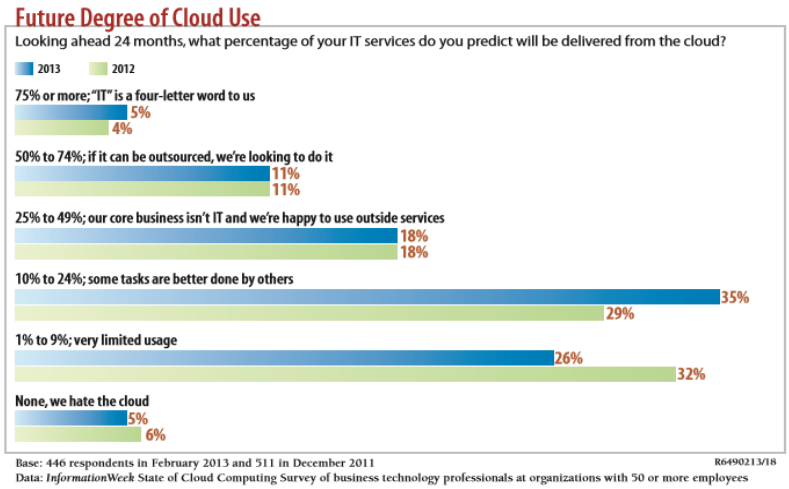


FIGURE 4.23 - Future Degree of cloud use

Source: InformationWeek 2013 State Of Cloud Computing

4.8.2 Security a Major Barrier in Cloud Adoption

The CDW's 2013 State of the Cloud Report, which involves 1,242 IT decision makers from various industries (Figure 4.24), revealed a similar result: the trend is upward, yet security concern remains the biggest impending factors to cloud among all the industry/participants across the board.

IT decision makers	Titles	Organization size
100% of respondents are familiar with their organization's use of, or plans for, cloud computing	12% Chief/Deputy CIO 7% Chief/Deputy CTO 45% IT Director/Manager 24% IT Supervisor/Specialist 12% IT Systems Engineer	13% Less than 50 employees 12% 50-99 employees 23% 100-499 employees 35% 500-10,000 employees 17% More than 10,000 employees

Small business (20-99 employees)	Medium business (100-499 employees)	Large business (500+ employees)	Federal government	State & local government	Healthcare	Higher education	K-12 public school districts
n = 155	n = 155	n = 157	n = 155	n = 155	n = 156	n = 157	n = 152
			61% Federal civilian 39% Department of Defense	51% State 38% County 11% Municipal	74% Hospital/ medical center 14% Doctor's office 12% Long-term care facility	46% Public four year 42% Private four year 10% Public community college 2% Private community college	

FIGURE 4.24 - CDW Survey: Participants' Demographics

Source: CDW's 2013 State of The Cloud Report

46% of the 1,242 respondents said security is the biggest barrier to cloud (Figure 4.25). The respondents are from small companies/organizations with less than 50 employees (13%) and larger organizations with 50+ up to more than 10,000 employees (Figure 4.24).

FIGURE 4.25 - CDW Survey: Biggest Impending Factors to Cloud

Source: CDW's 2013 State of The Cloud Report

Overall, what is the status of cloud computing within your organization?*

	Large business	Higher education	Small business	Federal government	K-12	Medium business	Healthcare	State & local government
Percentage of organizations implementing or maintaining cloud computing *2012*:	44%	43%	42%	42%	42%	40%	35%	27%
Percentage of organizations implementing or maintaining cloud computing *2011*:	37%	34%	21%	29%	27%	21%	30%	23%

FIGURE 4.26 - CDW Survey: Industry Cloud Adoption

Source: CDW's 2013 State of The Cloud Report

CDW's report, just like the InformationWeek's shows that less than 50% of the companies surveyed implement/utilize cloud, topping the list is the large business with 44% adoption rate to date while state and local government is still lagging at 27% (Figure 4.26). Overall, 39% of the respondents said that they are either currently implementing cloud computing within their organizations or maintaining it (Figure 4.27). While a wide variety of functions/applications has already been migrated to cloud - Messaging (18%), conferencing and collaboration services (17%), storage (15%), and Office/productivity suites (13%) (Figure 4.28) -, more than half of the organizations that were surveyed are still currently in the process of migration or planning to migrate various types of services to the cloud. Figure 4.29 shows the top services or applications that are moving to the cloud.

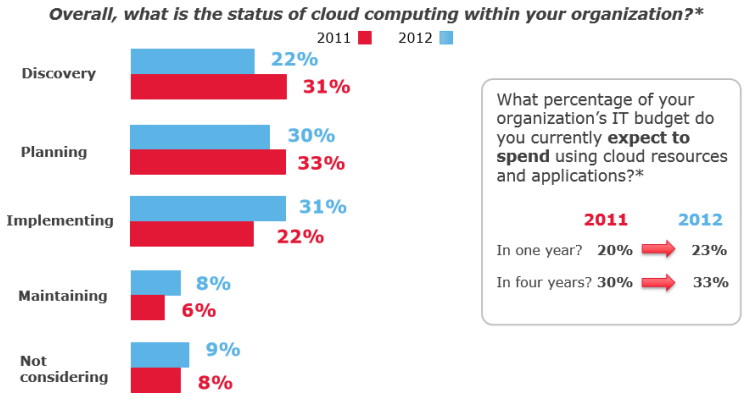


FIGURE 4.27 - Status of cloud computing

Source: CDW's 2013 State of The Cloud Report

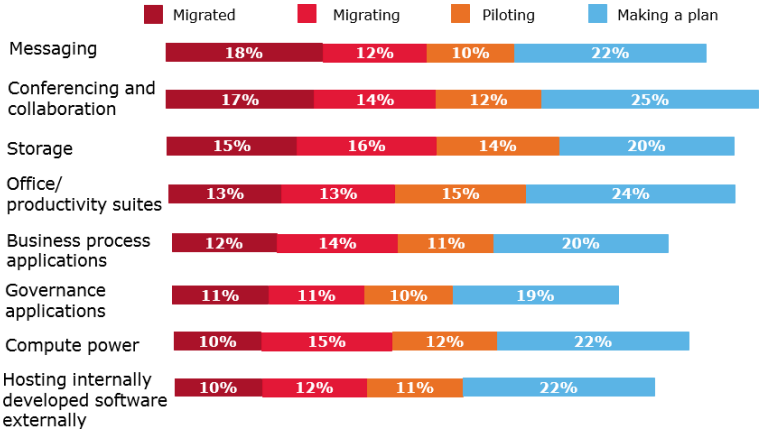


FIGURE 4.28 - What is moving to cloud

Source: CDW's 2013 State of The Cloud Report

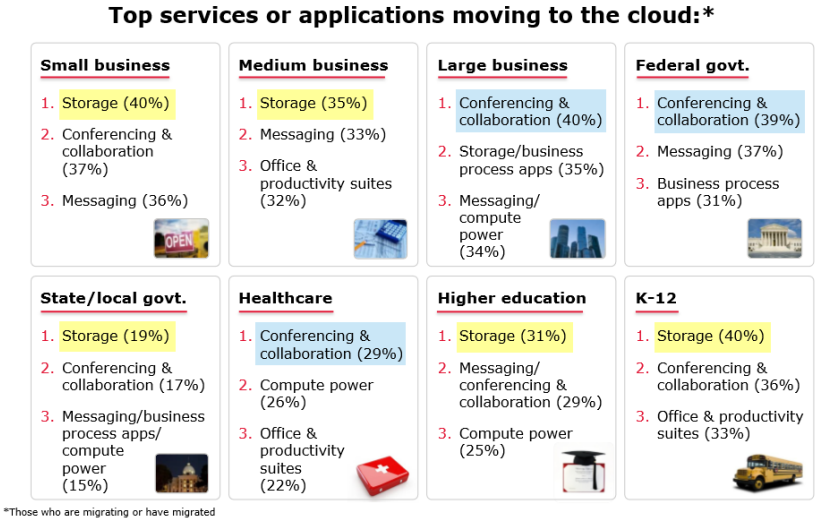


FIGURE 4.29 - Top services or applications moving to the cloud by Industry

Source: CDW's 2013 State of The Cloud Report

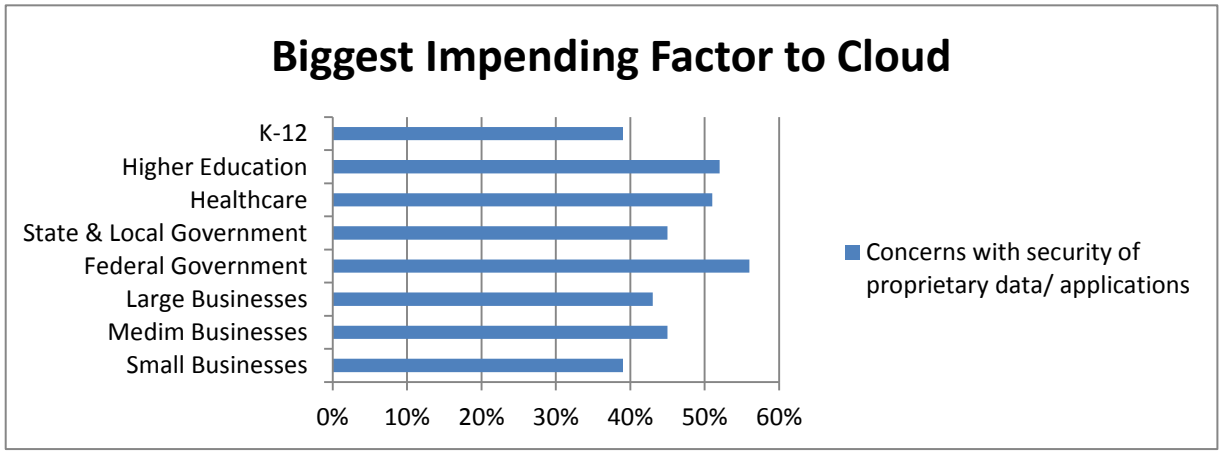


FIGURE 4.30 - Biggest impending factor to cloud

Source: CDW's 2013 State of The Cloud Report

The two surveys revealed similar results: while the cloud adoption is on upward trend, security concerns consistently emerge as a significant problem and considered to be the biggest barrier to cloud (Figure 4.30). The next section presents the specific technical security issues surrounding cloud based applications.

4.9 Cybercrimes and SaaS solutions Security Issues

The steady rise of reported incidents regarding security breaches, hacking, and unauthorized access to confidential data appear to have a negative effect on cloud adoption. The latest surveys on the state of cloud computing show that organizations have serious concerns on cloud security and that organization deem it as a significant barrier to cloud. In order to understand the validity of these security concerns and to find out whether technical security issues do exist, five industry expert reports were analyzed, each based on distinct methodologies which includes: internet traffic analysis, actual application security assessments, vulnerability assessments results (code analysis), data breach investigations (covering 19 countries), real time monitoring of global threat activities (covering 157 countries), and the result is conclusive: cloud users do have reason to be anxious of using cloud based services. This section presents the various technical issues of cloud computing, as this study focuses on SaaS, Issues that are related to Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) weren't covered.

4.9.1 2013 Data Breaches Report

In order to assure the relevance of a given problem, first, it is necessary to understand how serious the problem is. In Chapter 2, various security related incidents were cited, though the information came from reliable news organizations and were even confirmed by the companies involved, still those reports were based on how the reporters understood the incident rather than from a rigid and methodical study. This section presents the latest Data Breach Investigation Report (DBIR) of the Verizon trust team. This report is perhaps the most relevant and trusted report as it is commonly cited in the industry. The report is the result of collaborations between the Verizon's Risk team and the 18 diverse global organizations crossing international and public/private lines (Figure 3.1); the report covers 27 different countries (Figure 4.31).

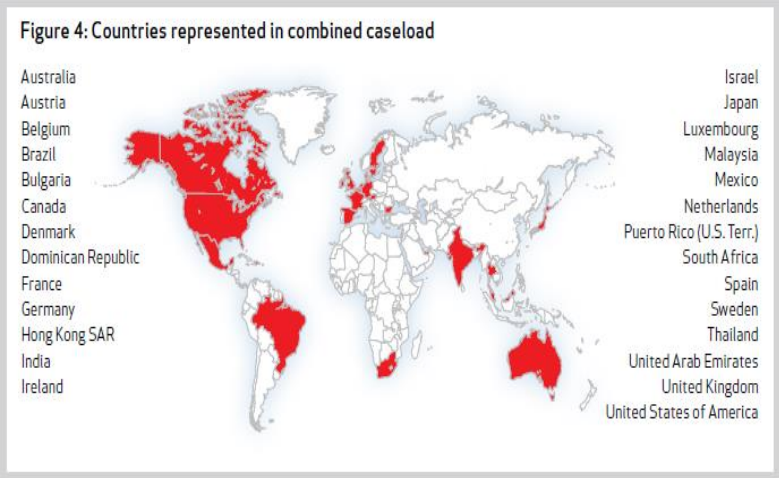


FIGURE 4.31 – Countries Represented in the combined case load

Source: Verizon's 2013 Data Breach Investigation Report

The 2013 DBIR recorded 47,000+ security incidents, 621 confirmed data disclosures and at least 44 million compromised records. The data breach were mostly due to financial reason, no wonder why the retail sector topped the list by a wide margin (21.7%) compared to the next which is manufacturing at 12.2% (Figure 4.32)

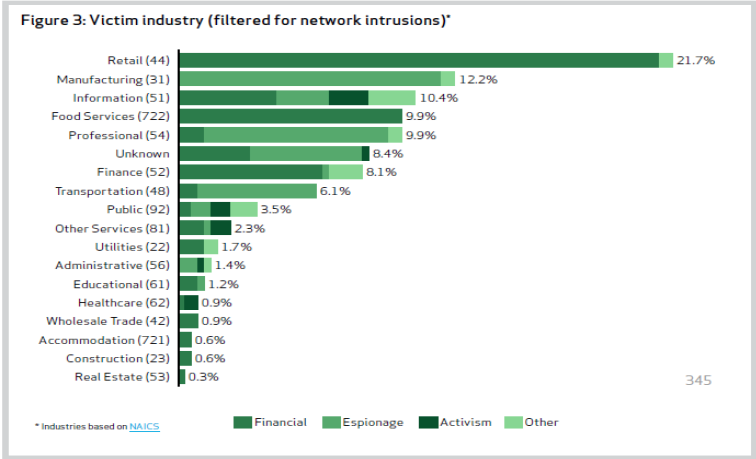


FIGURE 4.32 – Victim Industry

Source: Verizon's 2013 Data Breach Investigation Report

Considering that companies have more control over physical, environmental and operational security of their own network and computing devices, it's not surprising that most of these attacks were executed remotely; 76% of the data breaches were due to network intrusions, 52% from hacking, and 40% incorporated malware (Figure 4.5). Apparently, web application servers are the primary target as it is located in a demilitarized area within the companies' network (Figure 4.33); hence, unsecured web application can be seen as the favorite attack vector of hackers and intruders.

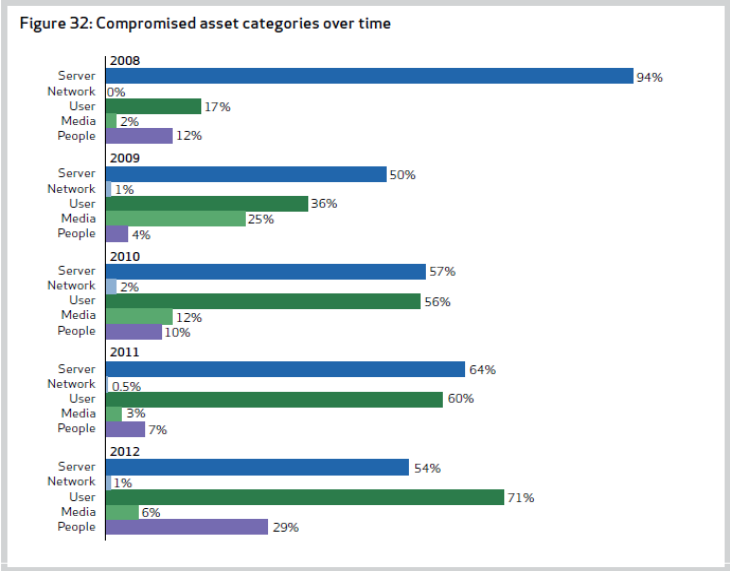


FIGURE 4.33 – Most Compromised Assets

Source: Verizon's 2013 Data Breach Investigation Report

Regardless of the size of the company, small or large (at least 1,000 employees), the overall source of attack is 92% external (Figure 4.34), this is expected as the majority of the attacks were performed from the outside targeting companies' servers and users; it suggests that in terms of SaaS based solutions, the threat emanating from the SaaS providers themselves (partner) are almost negligible (1%), which is what expected as trust is a critical factor in their relationship with their customers/clients; however, the significant threat coming from external sources (e.g. hackers) poses a real threat. Figure 4.35 shows that, overtime, the security threats that

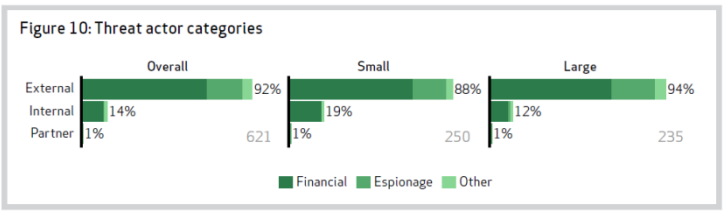


FIGURE 4.34 – Threat Actor Categories over time

Source: Verizon's 2013 Data Breach Investigation Report

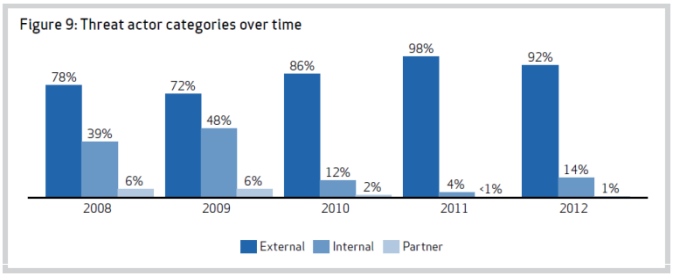


FIGURE 4.35 – Threat Actor Categories over time

Source: Verizon's 2013 Data Breach Investigation Report

originate from partner are going down while the external threats are going the opposite way.

In summary, the 2013 Report by Verizon found out that 92% of data breaches in 2012 covering 27 countries, were perpetrated by outsiders; 38% of the victims were considered large organizations (at least 1000 employees); the motivation was primarily financial (75%) targeting both the users (71% for 2012) and servers (54% for 2012).

FIGURE 4.36 – Top Causes of Data Breaches

Source: Symantec Internet Security Threat Report 2013

The 2013 Internet Security report by Symantec supports the DBIR report; it revealed that hackers were responsible for 40% of all data breaches in 2012 (Figure 4.36). It appears that the manufacturing was the top victim at 24% (Figure 4.37); the health sector is responsible in the 36% disclosed data breaches (Figure 4.38), there were 31 Million data breaches recorded in January (4.39). Symantec had observed almost 1/3 increased in web-based attack, 42% increase in targeted attacks or an average of 116 targeted attacks per day with 604, 826 average numbers of identities exposed per breach; the company also discovered 5,291 new vulnerabilities in 2012. (Symantec, 2013)

Regardless which report you look at, the data are consistent, cybercrimes driven by financial motives are on the rise; web based attack is prevalent; there seem to be no particular target as both small and large companies in various industries (Figure 4.37) across all sectors (Figure 4.38) could fall victim.

In order to quantify the effect of these data breaches or attacks to businesses, the next section looks at the cost of cybercrimes.

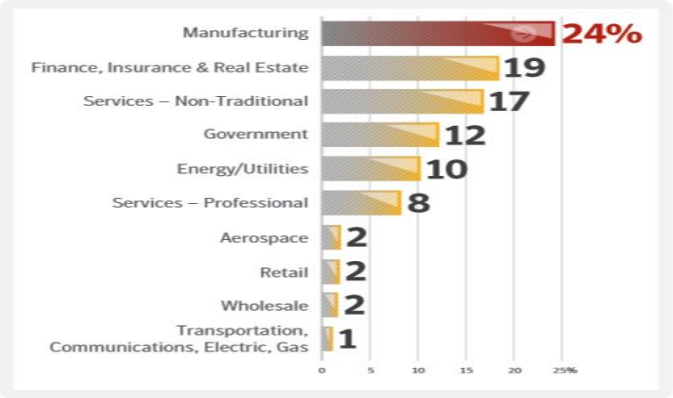


FIGURE 4.37 – Data Breaches by Industry

Source: Symantec Internet Security Threat Report 2013

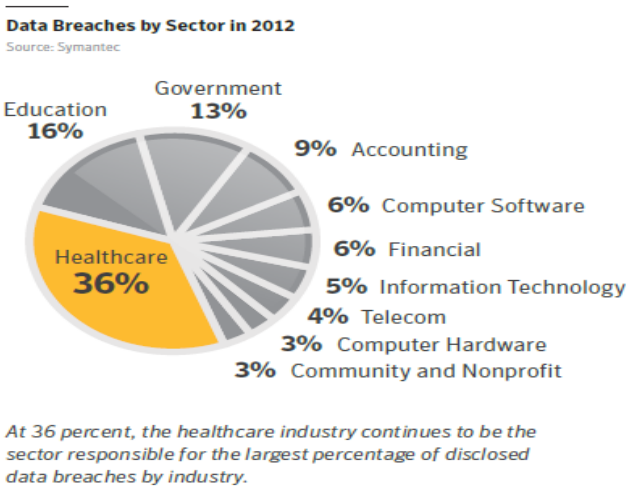


FIGURE 4.38 – Data Breaches by Sector

Source: Symantec Internet Security Threat Report 2013

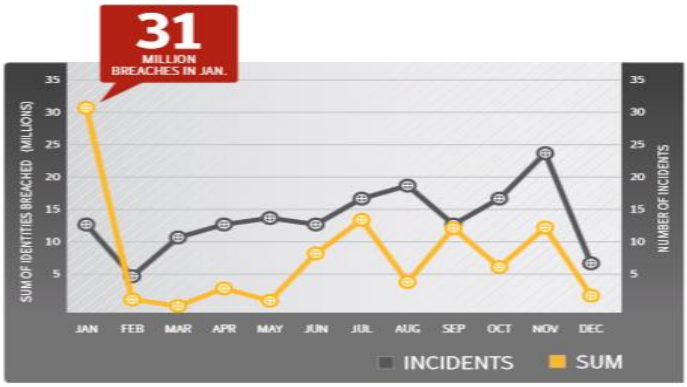


FIGURE 4.39– Data Breaches Incidents

Source: Symantec Internet Security Threat Report 2013

4.9.2 Cost of Cybercrimes

The study conducted by the Ponemon Institute concluded that cybercrimes continue to be costly, costing the 56 organizations that were participated their study an average of $8.9 million per year (Figure 4.40), a 6% increase from the 2011 survey (Figure 4.41). Symantec's data came up with a more specific figure putting the cost of a data breach to $194 average cost per capita. Apparently, the monetary cost of cybercrimes to companies, alone, is alarming, having to spend additional money on top of the budget allocated for IT and System security to cover the cost of cybercrime is oxymoron; the CIO or the head of the security, in case they find it necessary to include this item –cost of cybercrime- to the budget, would perhaps have a hard time explaining it to the board. If this trend continues, and the impact of cybercrimes span to other boundaries such as enterprises' trust to the cyberspace security, this could significantly affect the cloud industry.

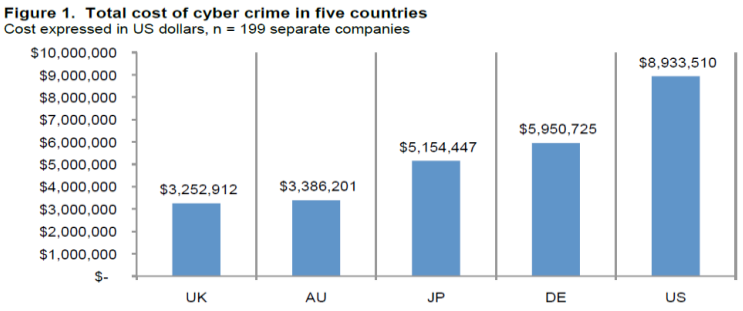


FIGURE 4.40– Total Cost of cybercrime in five countries

Source: 2012 Cost of Cyber Crime Study: United States

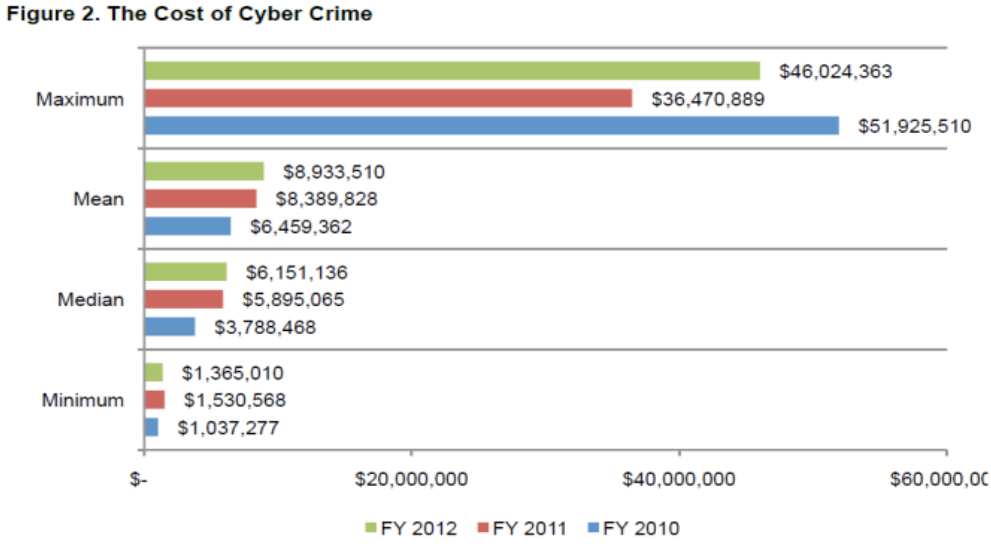


FIGURE 4.41– The cost of Cyber Crime 2010 - 2012

Source: 2012 Cost of Cyber Crime Study: United States

TABLE 4.6– – Average Cost Per Capita of a Data Breach

Source: Symantec Internet Security Threat Report 2013

Average Cost Per Capita of a Data Breach [6]

Source: Symantec

Country	Average Cost Per Capita
U.S.	$194
Denmark	$191
France	$159
Australia	$145
Japan	$132
UK	$124
Italy	$102
Indonesia	$42

At US$194, the United States is the country with highest in cost per capita, with Denmark a close second at $191 per capita.

Now that the high level technical issues of cloud based solutions, as well as the cost of successful cyber-attacks, have been established, the next step is to look at these issues in more detail; the following sections look at the most prevalent attacks on SaaS based solutions, and the top technical vulnerabilities of web applications

4.9.3 Most Prevalent Attacks on SaaS based solution.

A locally deployed application such as a custom designed Financial Management System that can only be accessed within the company's network is undoubtedly more secured compared to an application that is exposed to the World Wide Web. SaaS based solutions or applications that are delivered over the internet, because the application is exposed to the web, regardless of all the security features in place are arguably less secure, legitimate users and hackers alike could discover vulnerabilities on the application and use them to gain access to restricted data or resources on the server for financial or any other reasons. This section looks at the most prevalent attack that hackers use to access restricted data.

The Imperva's latest Web Application Attack Report, which is based on observing and analyzing internet traffic to 50 sample web applications during the past 6 months, revealed the following most frequently used attacks:

- SQL injection or SQLi (Maximum 320 attack incidents)
- Directory Traversal or DT (135)
- Remote File Inclusion or RFI (119)
- Local File Inclusion or LFI (55)
- Cross Site Scripting XSS (49)

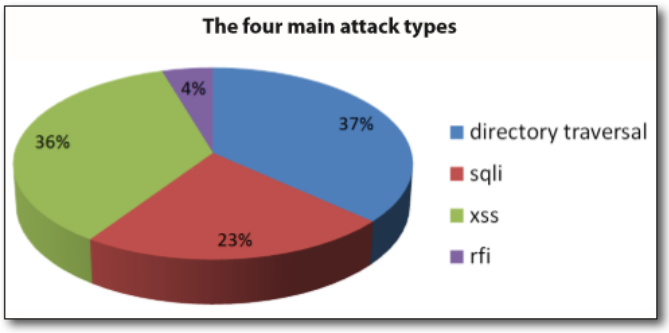


FIGURE 4.43– Most Prevalent Attack 2011

Source: Imperva's Web Application Attack Report Edition #3 - July 2012

Compared to any other types of attacks, SQLi appears to be the most commonly used. It had surpassed directory traversal which was the most prevalent type of attack in 2011 (Figure 4.43); this is not a surprise, Directory Traversal (DT) attack is not the most complicated attack type (see section 4.4.3, page 47), this vulnerability can easily be remedied from the server side without changing the application's source code. Figure 4.44 summarizes the result of the observation; this is based on applications that suffered significantly high volume of attack incidents: (the threshold used was more than 1000 malicious HTTP request in 6 months observation period). 18 apps for SQLi, 18 apps for RFI, 15 for LFI, 12 for Directory Traversal, 17 for XSS, and for business logic attacks, 10 apps for email extraction, and 5 apps for comment spamming.

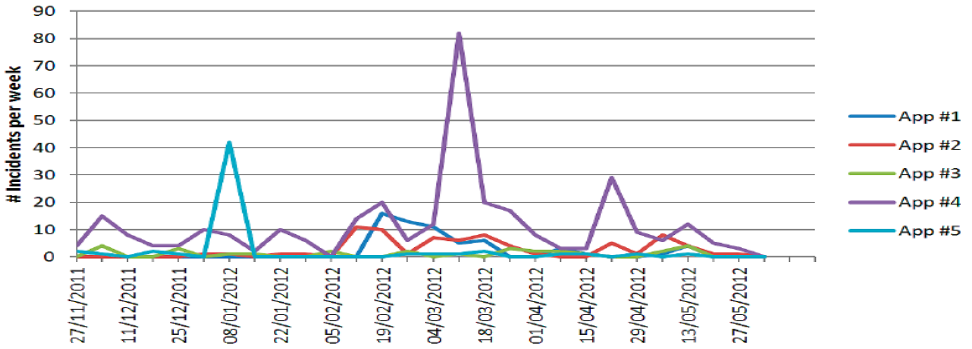


FIGURE 4.44 – SQLi attack incidents on top 5 applications which suffered the most attack

Source: Imperva's Web Application Attack Report Edition #3 - July 2012

TABLE 4.7– Amount of Incidents 2013

Source: Imperva's Web Application Attack Report Edition #3 - July 2012

Amount of attack incidents (incidents/6 months)							Amount of attack incidents (incidents/6 months)		
	SQLi	RFI	LFI	DT	XSS	HTTP		EmExt	ComSpm
Median	17.50	8.00	5.50	13.00	6.00	27.00	Median	3.50	7.00
Max	320.00	119.00	55.00	135.00	49.00	1359.00	Max	27.00	70.00
1st Quartile	8.00	2.00	3.75	6.00	1.25	8.00	1st Quartile	2.25	4.00
3rd Quartile	53.25	23.00	11.50	26.00	16.25	68.75	3rd Quartile	5.00	8.00

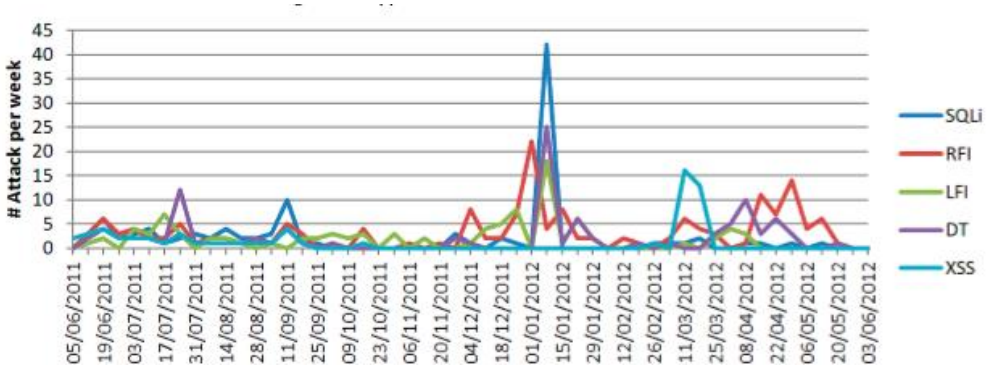


FIGURE 4.45– Single Application case Study for full year

Source: Imperva's Web Application Attack Report Edition #3 - July 2012

Figure 4.45 shows the absences of an attack pattern, although SQLi driven attack at some point reached above 40 level, this is not consistent, likewise the recorded spike on attacks that took place between the weeks 18 December 2011 to 12 January 2012 is just one off. But at the end, it is evident that there was an increased in attack incidents during the last 6 months or first half of 2012.

TABLE 4.8– Countries from which most attack requests were initiated (in thousands)

Source: Imperva's Web Application Attack Report Edition #3 - July 2012

RFI		SQLI		DT		LFI		EmExt		ComSpm	
Country	Requests (1000's)	Country	Requests (1000's)	Country	Requests (1000's)	Country	Requests (1000's)	Country	Requests (1000's)	Country	Requests (1000's)
USA	150	France	803	USA	342	USA	40	Senegal	14	Russian Federation	31
United Kingdom	47	USA	232	Canada	35	China	18	European Union	14	Ukraine	14
France	21	China	24	Germany	32	Germany	10	USA	10	Germany	9
Sweden	15	Netherlands	22	United Kingdom	18	France	10	Ivory Coast	8	USA	9
Germany	11	Mexico	21	Ukraine	9	Canada	9	Malaysia	4	China	8
Canada	9	Bulgaria	15	Brazil	7	Brazil	7	Italy	3	Latvia	8
Spain	8	Albania	10	China	6	Poland	7	Nigeria	2	United Kingdom	4
Italy	7	Ukraine	9	Japan	5	United Kingdom	5	Ghana	2	Poland	2
Turkey	5	Germany	9	France	5	Italy	5	Germany	2	Netherlands	2
Netherlands	4	United Kingdom	8	Russian Federation	3	Colombia	5	Thailand	1	France	2

USA, western European countries, China, and Brazil, topping the list of countries where the most prevalent attack initiated (Table 4.8), are not a surprise. However, perhaps for some, it is surprising to see western African countries, like Senegal, Nigeria, Ghana, and the Ivory Coast to top the list of the email extraction attack type originator.

The report confirms that web applications or SaaS based solutions in general, do have technical security issues: SQLi, DT, RFI, LFI and XSS being the most prevalent types of attack used. Although SQLi is the most commonly used attack type for 2012, there is no attack pattern observed and that attack incidents could spike at a particular period; USA is

still by far (based on external IP) is the primary source of attacks topping the following attack types: RFI, DT and LI.

4.9.4 Most prevalent web application vulnerability

Security experts and professionals alike agree that absolute online security cannot be guaranteed; however, it can be argued that a highly secured web application could significantly deter hackers from executing their attack plans. This section looks at the top vulnerabilities of web applications and the current state of website security from WhiteHat's expert's perspective.

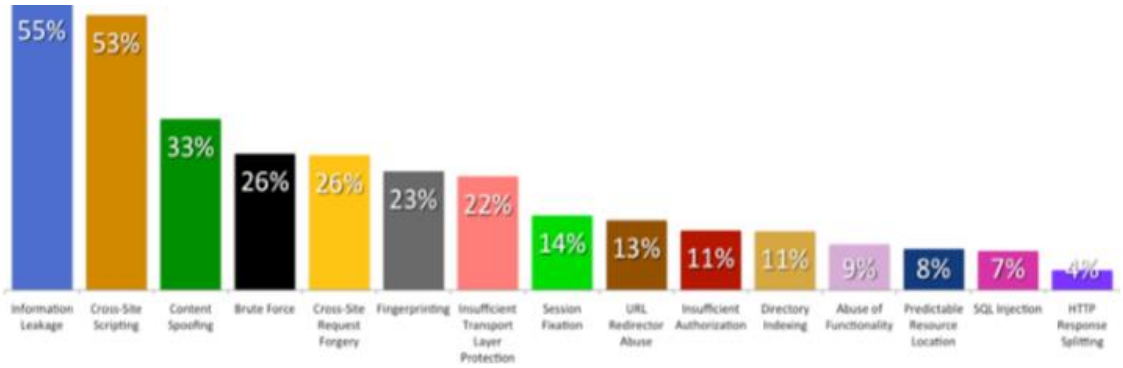


FIGURE 4.46– Top 15 Vulnerability Classes (2013 report)

Source: WhiteHat's Website Security Report- May 2013

Unlike the Imperva's report, WhiteHat's is based on actual vulnerability assessment, the organization maintain a huge amount of vulnerability assessment data (hundreds of terabytes in size), which is the results of their assessments of "tens of thousands of websites across hundreds of the most well-known organizations" (WhiteHat, 2013). The report focuses on the vulnerabilities on web applications rather than the most exploited vulnerabilities. While

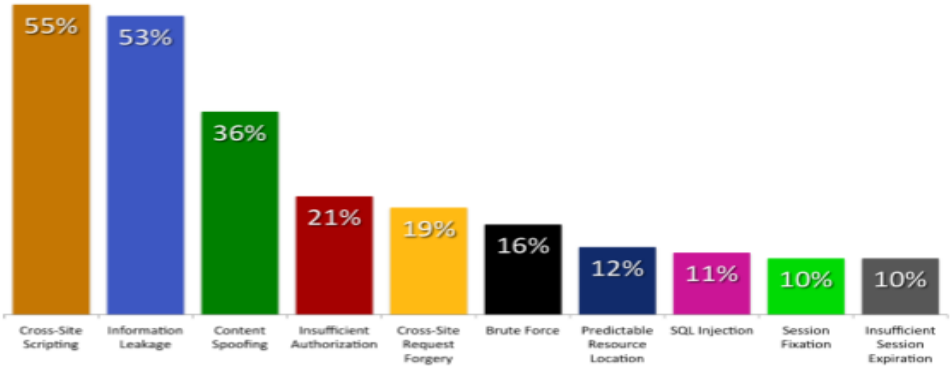


FIGURE 4.47– Top Vulnerability classes (2012 report)

Source: WhiteHat's Website Security Report- Summer 2012

Imperva's report suggest that SQL Injection is the most prevalent attack used (section 4.9.3, page 63); WhiteHat's latest report shows that SQL Injection (SQLi) only accounts for 7% (Figure 4.46) of total vulnerabilities on all the web applications analyzed; this suggest that vulnerability prevalence does not automatically correlate to vulnerability exploitation. However, the most prevalent attacks correlates to the remediation actions of developers' as what the data shows: SQLi is now at 7% it was 11% (Figure 4.47) in 2012 report 3% down from 14% (Figure 4.48) level in 2011, which means half of these vulnerabilities were already addressed in just two years, while the most prevalent vulnerabilities which are not commonly exploited are hardly changed.

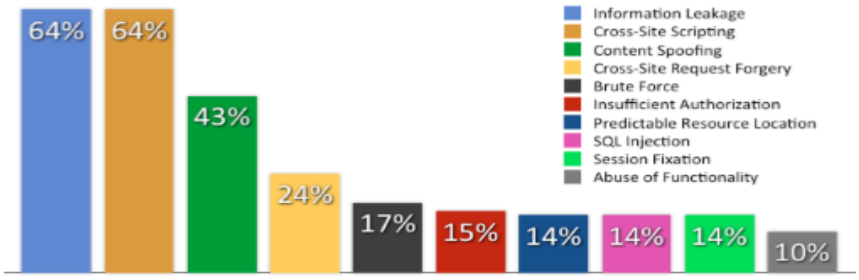


FIGURE 4.48– Top Vulnerability classes (2011 report)

Source: WhiteHat's Website Security Report- Winter 2011

Looking at the current state of website security (2013 report), 86% of all websites who were included in the report have one or more vulnerabilities and what is alarming is that important industries/sectors such as the Government, Manufacturing, Education, Energy, and Food & Beverage have 100% vulnerabilities (Table 4.10). While the remediation rate is above 50% the average time to fix rate is considerably long (e.g. 342 days for Education), perhaps at this rate –time to fix -, hackers have already discovered another vulnerabilities that they could use the next time they attack. In fact, looking at the previous two years reports (Tables 4.10 and 4.1), though the annual average vulnerabilities is on downward trend, it does not corresponds to the remediation rate meaning either new vulnerabilities were introduced or detected after a fix has been implemented.

TABLE 4.9 – The current state of website security (2013) by industry

Source: WhiteHat's Website Security Report- May 2013

Industry	Avg Vuln Sites	Annual Avg Vulns	Remediation Rate	Avg. Time-to-Fix (Days)
All	86%	56	61%	193
Entertainment & Media	91%	12	81%	33
Financial Services	81%	50	67%	226
Retail	91%	106	54%	224
Technology	85%	18	61%	71
IT	85%	114	54%	185
Healthcare	90%	22	53%	276
Banking	81%	11	54%	107
Manufacturing	100%	27	55%	197
Social Networking	86%	20	46%	175
Telecommunications	89%	20	74%	163
Education	100%	47	58%	342
Energy	100%	59	71%	144
Insurance	78%	39	55%	274
Government	100%	8	65%	48
Non Profit	95%	28	41%	236
Food & Beverage	100%	18	46%	36
Gaming	92%	17	46%	67

TABLE 4.10 – The current state of website security (2012) by industry

Source: WhiteHat's Website Security Report- Summer 2012

Industry	Annual Avg. Vulnerabilities	Std. Dev	Avg. Time-to-Fix (Days)	Average Remediation	Std. Dev	Window of Exposure (Days)	Std. Dev
ALL	79	670	38	63%	36	231	159
Banking	17	554	45	74%	37	185	147
Education	53	885	30	46%	37	261	153
Financial Services	67	853	80	63%	35	227	157
Healthcare	48	461	35	63%	36	239	155
Insurance	92	171	40	58%	32	211	154
IT	85	36	35	57%	31	208	159
Manufacturing	30	56	17	50%	33	252	125
Retail	121	125	27	66%	36	238	160
Social Networking	31	431	41	62%	43	264	162
Telecom	52	82	50	69%	31	271	136
Non-Profit	37	56	94	56%	40	320	168
Energy	31	62	4	40%	35	250	154

TABLE 4.11 – The current state of website security (2011) by industry

Source: WhiteHat's Website Security Report- Winter 2011

Industry	Number of Vulnerabilities	Std. Dev	Remediation Rate	Std. Dev	Window of Exposure (Days)
Overall	230	1652	53%	40%	233
Banking	30	54	71%	41%	74
Education	80	144	40%	36%	164
Financial Services	266	1935	41%	40%	184
Healthcare	33	87	48%	40%	133
Insurance	80	204	46%	37%	236
IT	111	313	50%	40%	221
Manufacturing	35	111	47%	40%	123
Retail	404	2275	66%	36%	328
Social Networking	71	116	47%	34%	159
Telecommunications	215	437	63%	40%	260

In terms of the overall exposure to serious vulnerabilities, it looks like websites security across all industries represented in WhiteHat's study is in a serious state. The latest report

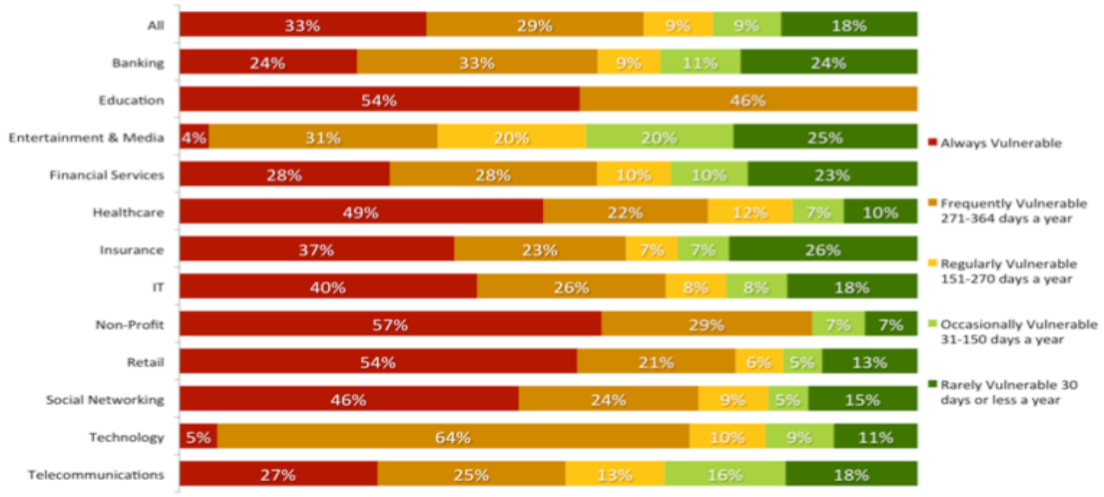


FIGURE 4.49 – Overall Window of Exposure to Serious Vulnerabilities (2013)

Source: WhiteHat's Website Security Report- May 2013

revealed that 33% of all websites are always vulnerable, 29% frequently vulnerable within 271-363 days a year, only 18% are rarely vulnerable 30 days or less a year (Figure 4.49). As there is no way WhiteHat will reveal the identities of these websites, it is perhaps safe to say that 3 out of 10 websites that internet users visit on a daily basis have vulnerabilities; Figures 4.50 and 4.51 shows the 2012 and 2011 results.

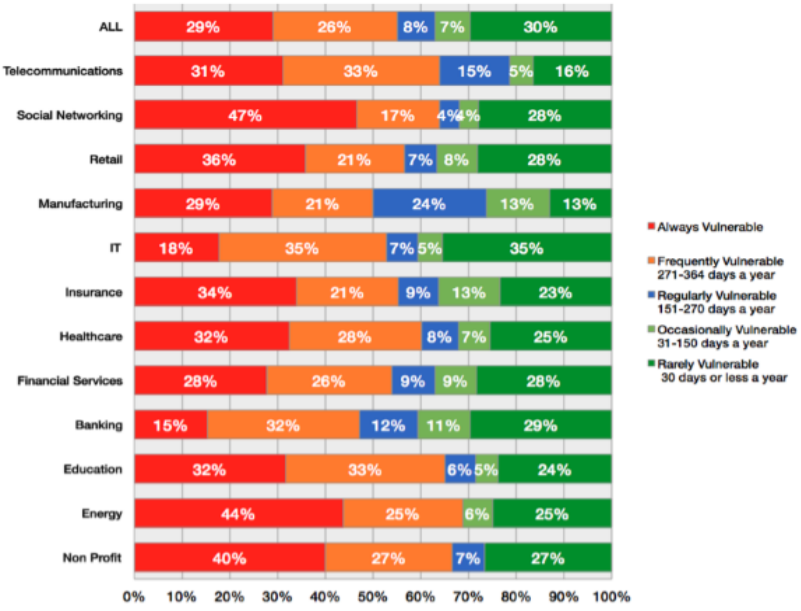


FIGURE 4.50 – Overall Window of Exposure to Serious Vulnerabilities (2012)

Source: WhiteHat's Website Security Report- Summer 2012

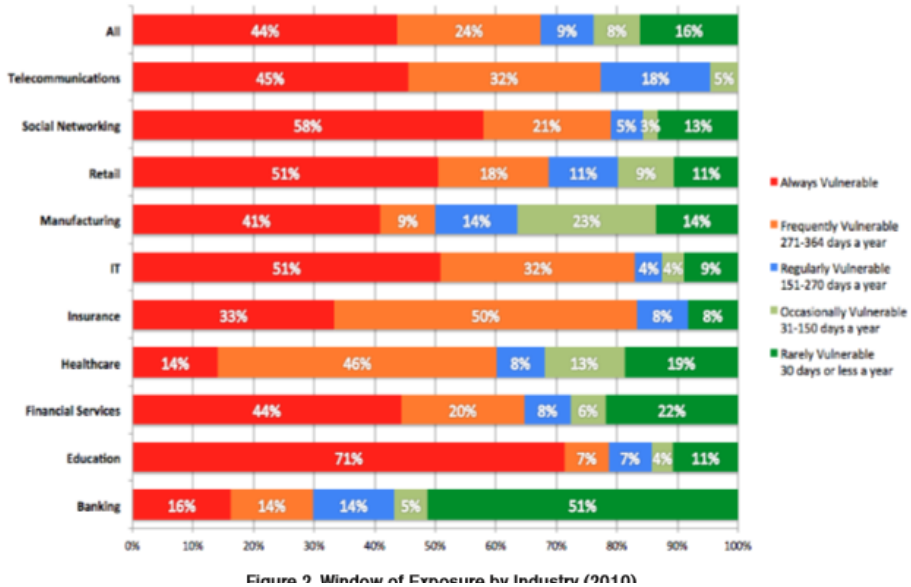


FIGURE 4.51 – Overall Window of Exposure to Serious Vulnerabilities (2011)

Source: WhiteHat's Website Security Report- Winter 2011

In summary, the state of website security is not looking good, 33% -always vulnerable website across all sectors- is a significant number and cannot be ignored. While developers were able to address vulnerabilities 61% of the time, the time to fix which could take up to almost a year (342 days) seem too long. The prevalence of vulnerability does not correlate to the commonly exploited vulnerabilities. In the case of WhiteHat security report, the most prevalent vulnerabilities are: Information Leakage, Cross Site Scripting and Content Spoofing; these vulnerabilities continuous to top the list for three years now. The next section digs deeper into the subject, it looks at the root cause of data breaches (validate the previous data for triangulations), code security compliance of application providers/developers, and the vulnerability distribution at the lowest level (Programming Language).

4.9.5 State of Software Security

Just like desktop applications, web based applications or Software as a Service (SaaS) are also written in a specific programming language such as Java for J2EE and CSharp or VB for .NET platform. The only difference is that desktop applications are locally deployed and users usually interact with it using a custom graphical user interface while SaaS based are accessible via the internet and normally exposed to the entire internet population for mass consumption. This section dissects the Veracode's State of Software Security Report. The report is based on actual application security assessments conducted to identify vulnerabilities and validate remediation, the latest report, now volume 5, examines data

collected from January 2011 through June 2012 (18 months), representing 22,430 application builds that were uploaded to the Veracode's platform for assessment.

In terms of the root cause of data breaches, the Veracode report agrees with Verizon's Data Breach and Symantec's report, 45% (Figure 4.52) according to the Veracode, DataLossDB being its source, is due to hacking. This is not surprising at all, as more and more services migrate to the cloud, the opportunity to benefit through misuse of these services increases; also as hacking knowledge proliferates and with a freely open cyberspace, there is no doubt that the hacking community will continue to grow, resulting to a more severe problem on data breaches.

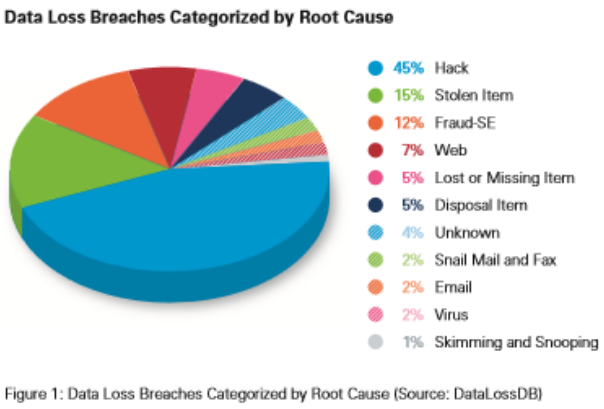


Figure 1: Data Loss Breaches Categorized by Root Cause (Source: DataLossDB)

FIGURE 4.52 – Data Loss Breaches by Root Cause

Source: Veracode's State of Software Security – April 2013

While the growing pool of hackers and the proliferations of hacking information and tools cannot easily be controlled, the security of the application or services that are migrated to the cloud be an effective deterrence against hackers. The question is how are software development companies/application providers are doing to deter attacks? Veracode's report answers this question: they are not doing well. In terms of Enterprise, there is 70% non-compliance (Figure 4.53); this is 10% higher than last year's compliance rate (4.54). In terms of Web Application which uses OWASP Top 10 compliance standard -OWASP Top 10 is one of the standards used by PCI Data Security Standards (PCI DSS) to determine if an application is secure enough to process credit card data -, the result is much more upsetting as 77% of Web Applications submitted for OWASP Top 10 validation failed (Figure 4.55). Considering that

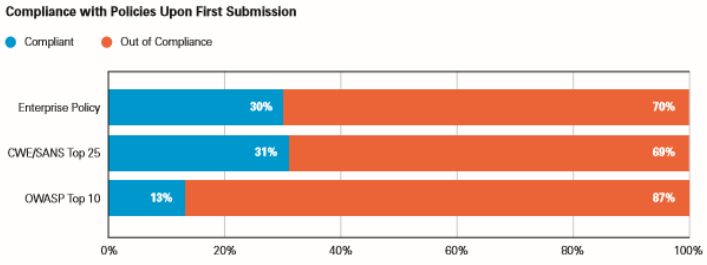


FIGURE 4.53 – Code Security Compliance (Volume 5 April 2013)

Source: Veracode's State of Software Security

this report is now volume 5 and the compliance level is still low suggest that developers or software providers are either falling behind in terms of code security or they just do not have a credible security QA team that assures compliance on this area.

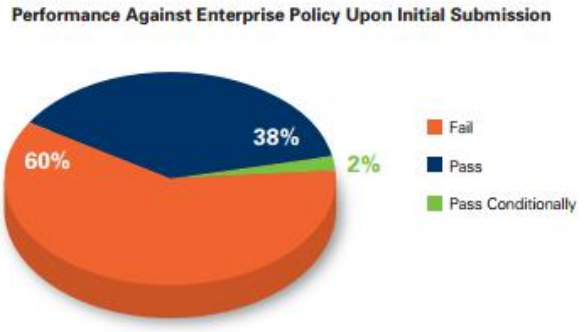


FIGURE 4.54 – Code Enterprise Policy Compliance (Volume 4 December 2011)

Source: Veracode's State of Software Security

Looking at the vulnerability distribution per platform, Cross Site Scripting (XSS) seem to be a major problem for applications written in all major programming languages, except for .NET. Although in general, some effort to address XSS issue could be observed, the effort was not enough to bring down XSS to the list.

Veracode's report appears to complement WhiteHat's as it also found XSS and Information Leakage to be the most prevalent vulnerabilities among web applications. Content Spoofing which also belongs to WhiteHat's top 3 is not included in Veracode's report because it is not a server side vulnerability (content spoofing is HTML/JavaScript vulnerability). Comparing the results of Veracode's last 3 reports (volumes 3-5), although some changes could be observed, there were no significant positive changes recorded, some vulnerabilities such as CRLF Injection even went up to 21% in volume 5, compared to only 16% in volume 4.

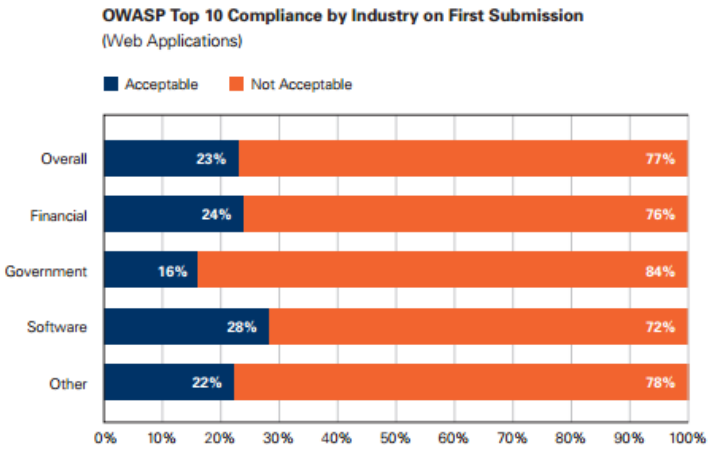


FIGURE 4.55 – OWASP Top 10 Compliance (Volume 4 December 2011)

Source: Veracode's State of Software Security

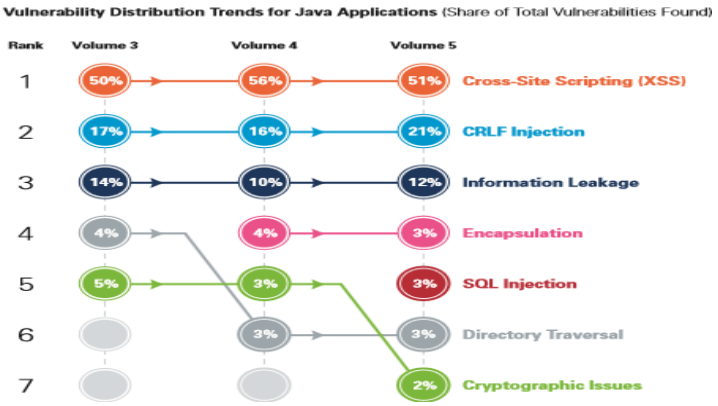


FIGURE 4.56 – Vulnerability Distribution Trends for Java Applications

Source: Veracode's State of Software Security – April 2013

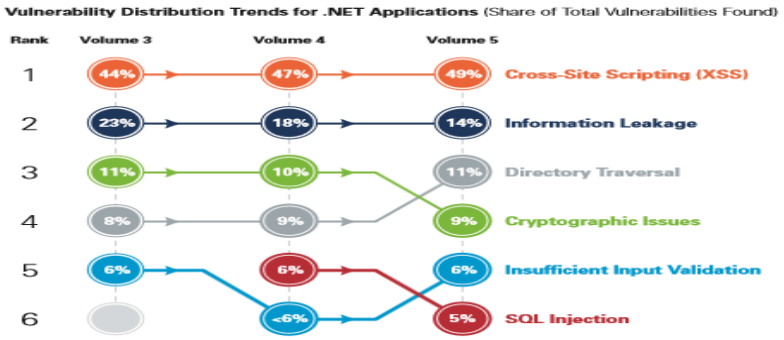


FIGURE 4.57 – Vulnerability Distribution Trends for .NET Applications

Source: Veracode's State of Software Security – April 2013

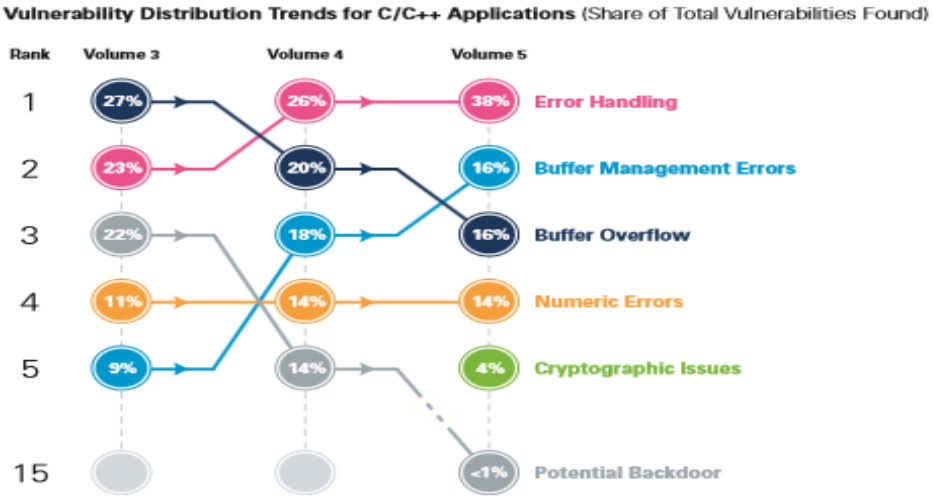


FIGURE 4.58 – Vulnerability Distribution Trends for C/C++ Applications

Source: Veracode's State of Software Security – April 2013

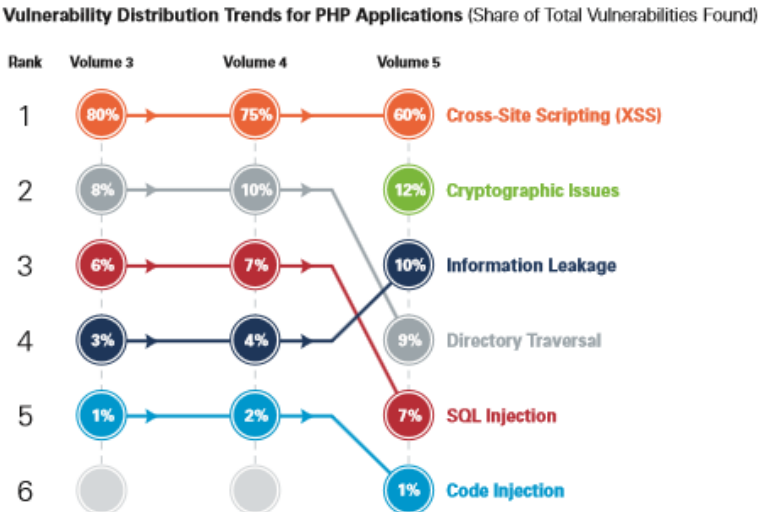


FIGURE 4.59 – Vulnerability Distribution Trends for PHP Applications

Source: Veracode's State of Software Security – April 2013

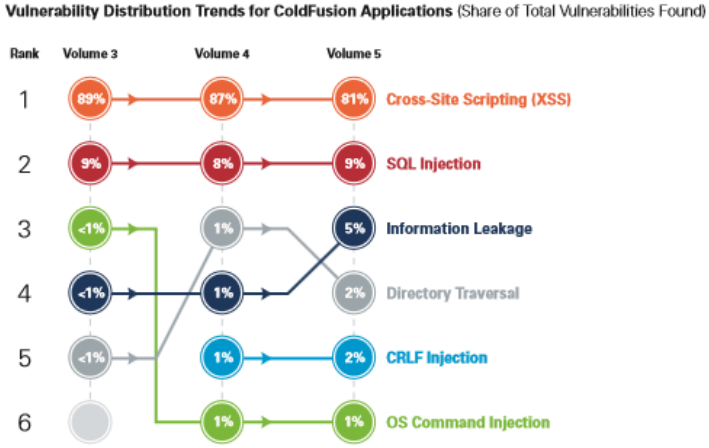


FIGURE 4.60 – Vulnerability Distribution Trends for ColdFusion Applications

Source: Veracode's State of Software Security – April 2013

The Veracode's vulnerability distribution lists (Figures 4.56 to 4.59), offer a really good and detailed insight of where the vulnerabilities lie; as the above figures suggests, application codes that were written on major programming languages have plenty of technical vulnerabilities waiting for hackers to exploit. Considering that developers and/or software houses' security compliance is low, there is a chance that these vulnerabilities will remain untouched.

Finally to validate the data gathered from all the reports that have been reviewed in this chapter, the next section looks at the Trustwave's Global Security Report.

4.9.6 Trustwave 2013 Global Security Report

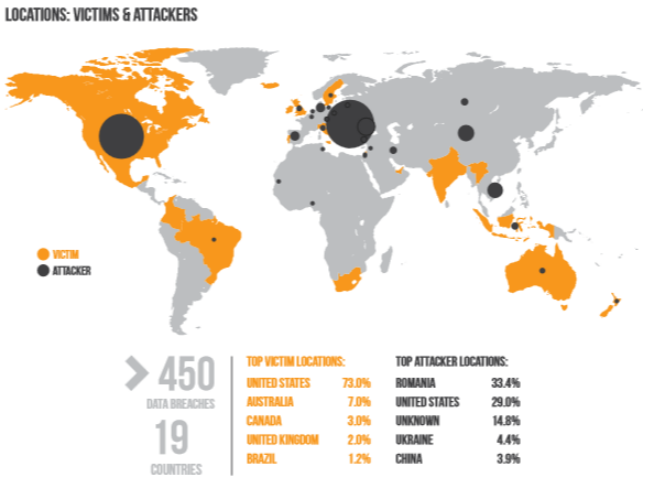


FIGURE 4.61 – Location of Victims and Attackers

Source: TrustWave 2013 Global Security Report

Unlike all the other reports, Trustwave conducts actual technical testing and analysis, the company's goal is to discover the top vulnerabilities that pose serious threat to organizations. This year's report is based on the 450 data breaches in 19 countries (Figure 4.61) that Trustwave had investigated.

It appears that the attackers target customer's record such as: payment card data and email addresses (Figure 4.62), USA topped the list of victim's location this is undoubtedly due to the fact that majority of online payment transactions are processed via US based servers. The attackers appears to had originated from 29 different countries, having the majority originated from Romania (33.4%), however since the data were based on the attackers' IP addresses this is inconclusive as there is a possibility that the actual attacks had originated somewhere else rather than the countries listed in the list.

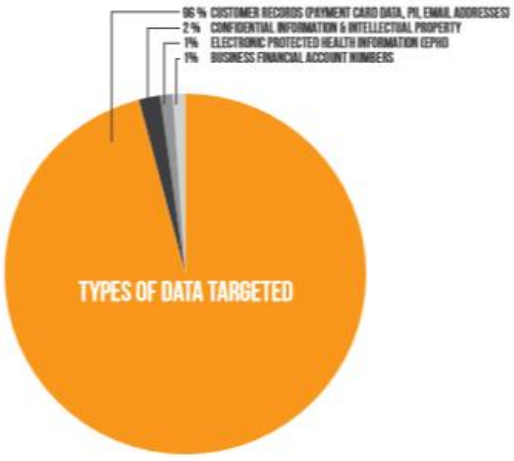


FIGURE 4.62 – Types of Data Targeted

Source: TrustWave 2013 Global Security Report

The Web Application Consortium's (WASC) Web Hacking Incident Database (WHID) where Trustwave based the data seem to agree with Imperva's report, SQLi which Imperva claimed to be the most prevalent attack also appear on WHID top 3 in both the 2011 and 2012 reports. But what is interesting about Trustwave report is that it suggests that the majority of attack methods used in the past 2 years were unknown (34% in 2011 and 46% in 2012 - Figure 4.63); this is alarming because

the fact that the remediation time for the known exploits are already long, there is a possibility that hackers are also exploiting these unknown vulnerabilities.

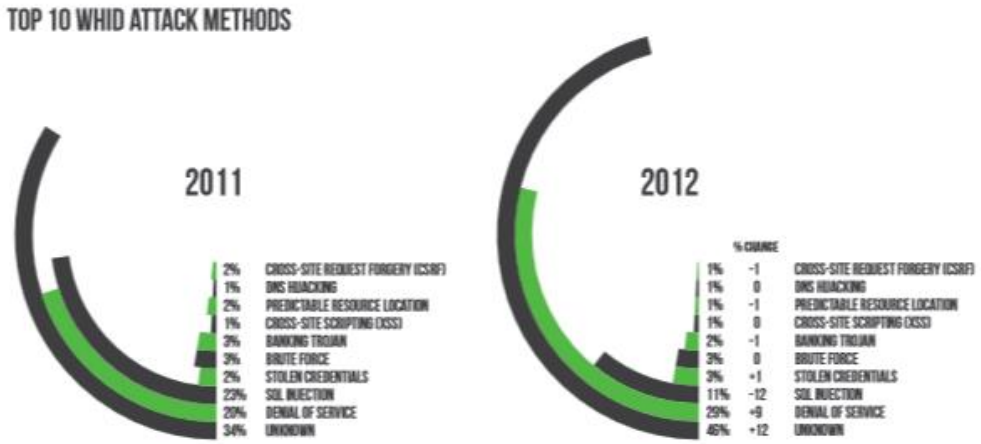


FIGURE 4.63 – Top 10 WHID Attack Methods

Source: TrustWave 2013 Global Security Report

TABLE 4.12 – Top 10 Application Vulnerabilities

Source: WhiteHat's Website Security Report- Winter 2011

Top 10 Application Vulnerabilities		
RANK*	Finding	Percentage of Applications Containing Vulnerability
1	SQL Injection	15%
2	Miscellaneous Logic Flaws	14%
3	Insecure Direct Object Reference	28%
4	Cross-Site Scripting (XSS)	82%
5	Failure to Restrict URL Access	16%
6	Cross-Site Request Forgery	72%
7	Other Injection	7%
8	Insecure File Uploads	10%
9	Insecure Redirects	24%
10	Various Denial of Service	11%

In summary, Trustwave's report appears to confirm the findings of the various reports that were analyzed and discussed in the previous sections. The attacks which originate from 29 different countries that targets customer's data had resulted to 450 data breaches in 2012; 46% of the attack methods used in 2012 was unknown but regardless of the attack methods used the vulnerabilities on web application (Table 4.12) are the major culprit of these cyber-attacks and data breaches.

4.10 Summary

The threats are real, cybercrimes are on the rise and continue to be costly, as the figures show that both cloud based data and applications aren't safe against attackers, cloud users have all the reason to be anxious about migrating to the cloud.

The problem seem to be multifaceted, it not just due to the growing population of the hacking community nor simply a software houses/developers security compliance issue. While the root of the problem appears to be unsecured applications – applications that contains substantial amount of vulnerabilities – that manage to reach the live environment, there are many other factors that contributes to the problem such: as lack of reliable Security Quality Assurance testing, security training for users, reliable IP tracking system, unsecured cyberspace among others.

Despite all the security vulnerabilities that most SaaS based applications have, it looks like enterprises' are still keen to utilize cloud based services, however, companies are aware that security is a real concern and there were indications that it had started to affect cloud adoption, as to when we can expect to see the full effect of the increasing problem on security to cloud adoption: not too soon. The increasing vulnerabilities on web applications that are currently in operation, the growing population of the hacking community and their increased hacking activities, the growing number of attack methods that are unknown and the rising cost of cybercrimes, if not addressed by cloud computing stakeholders, could soon affect the trust level of the enterprises to the cloud and thus could have a negative effect on cloud adoption.

5. Conclusions and Future Work

5.1 Introduction

The statistics show that cloud computing is a significant development in the current digital age. Surveys confirm that more and more company are migrating to the cloud, from a simple HR Time System to the more complicated ERP systems, are all going to the cloud. This is actually expected as building maintaining a pool of in-house applications cost companies significant amount of resources.

Cloud computing has challenges, first, cloud services are delivered over an unsecured and chaotic medium (the Internet) where cybercriminals operate; second, software providers or developers do not seem capable of delivering secured or clean code as most of the live applications have overwhelming number of technical vulnerabilities; third, although many applications vulnerabilities that exist on web applications are known and could be fix, the remediation time takes long (342 days for some industries) giving hackers more than enough time to exploit them, no wonder why data breaches are going up and hacking incidents are prevalent; lastly, while everyone agrees that the Internet or the cyberspace has now become a risky place where all sorts of illegal activities can happen undetected, there is no formal monitoring and policing system in place, there is no concept of border control and regulatory jurisdiction is not clear.

Regardless of all the technical vulnerabilities and security issues of cloud computing, the numbers are still positively in favor of the cloud. The adoption trend is still on upward track, however, surveys also show that businesses consider security a significant barrier to cloud, the enterprises' negative perception on cloud security is shared across all industries, if this perception remained, the trend could go the opposite direction.

5.2 The barriers to cloud adoption

Cloud providers are aware that cloud security is a major concern for their customers. Looking at their effort to assure users that business transactions and data that are held in cloud are safe; major cloud service providers such as SalesForce, Amazon, Google, Microsoft, IBM, Oracle; seem to be doing great. However, the various security reports that were reviewed in Chapter 4 revealed a different story, cybercrimes are on the rise and increasingly costly; multi-national companies are not immune from cyber-attacks, web applications have serious vulnerabilities, and unlike what cloud providers are saying, the result of expert reports

(Veracode, 2013) (Trustwave, 2013) suggest that software companies are not doing enough to address the problem.

From the application code level, a lot of technical vulnerabilities have been observed, Cross Site Scripting (XSS), Directory Traversal (DT), Information Leakage (IL), SQL Injection, CRLF Injection are some of the most prevalent vulnerabilities at present. WhiteHat's report which suggests that 86% of all web applications across all industries have one or more of these vulnerabilities are alarming, as this means that 8 out of 10 web applications that were analyzed have vulnerabilities, while the identities of these web applications and companies weren't divulge, it is safe to say that many of today's widely used applications have vulnerabilities – LinkedIn, Yahoo, Facebook, Microsoft, Apple, PayPal, MasterCard are only some of the companies that reportedly fell victims of cyber-attacks -.

While there are many other technical issues that contributes to the vulnerability of companies' security system, because web applications opens the companies' server to the whole world, these code level vulnerabilities are considered to be the primary culprit. Hackers normally exploit these vulnerabilities to bypass the target company's defense system. For example Imperva's report show that SQL Injection (SQLi), Directory Traversal (DT), Remote File Inclusion (RFI),Local File Inclusion (LFI), Cross Site Scripting (XSS) are the most exploited vulnerabilities; the remediation time which relatively long (in some industries takes up to 342 days), is also a problem, it gives hackers more than enough time to discover and exploit the vulnerabilities to bypass system security and get access to the restricted data/resources.

Surveys (CDW, 2013), (InformationWeek, 2013) show that while in general, users seem to disregard security in favor of the benefits of cloud based services, they considered it [security] to be a major barrier to cloud adoption. The expanding community of hackers and the increasingly unsafe cyberspace, while also an important issue, do not appear to be a significant factor; but cloud users expect the cloud providers to be capable of maintaining the security of their data and every transaction done via cloud.

One of the most effective ways to maintain cloud users trust to cloud services is eliminate or lessen the technical vulnerabilities on web applications. Having the confidence that it is safe to click any button on any web applications and that hackers have a very slim chance to discover and exploit any vulnerability on a web application, could significantly improve user's perceptions about cloud security. But until surveys, reports, analysis, studies and testing

show a positive sign of increased code security -total eradication of all these vulnerabilities, fast response time and high compliance on security policies-, regardless what the cloud providers say, application security will remain a major barrier to cloud adoption.

5.3 The future of cloud based computing

The figures show that while cloud adoption is on upward trend enterprises' are increasingly anxious about cloud security. It took Outsourcing two decades to achieve mainstream adoption, cloud computing is now more than a decade old, there is a possibility that mainstream adoption could be achieve in the next five years; however, considering that enterprises are increasingly concerned about security, there is also a risk of failure. Furthermore, the occurrence of a major security incident could have a significant and immediate impact to cloud adoption.

In today's digital age, anything can instantly become obsolete, industry could rise really fast (e.g. social networking) and diminish quickly (e.g. record stores); when a better solution emerge, it disrupts the status quo and creative destruction follows. If you analyze cloud computing in the context of SaaS based solutions (software delivered over the internet), you will realize that it provides most if not all what an enterprise need to operate with agility in the most cost effective way. For example, companies need the following: an enterprise class application, reliable infrastructure, fast access to data and applications, high quality redundancy systems, capable software developers, application operators, IT experts and many other resources to run and maintain a reliable IT system, while large companies are capable of having all these in-house, it comes with a price, medium and small companies would certainly find it financially challenging if not impossible to acquire. With cloud computing, any companies including the small ones can easily get access to all of these resources at a reasonable cost (e.g. ERP system from SalesForce only cost $20 per user/month), it apparently does not require cost and benefit analysis 20/user/month for an enterprise class ERP running on a highly reliable infrastructure supported by high caliber engineers, is a very compelling business case. Apparently this is just one of the many benefits of a SaaS based solution that undoubtedly makes cloud computing popular and made user disregard their security concerns. Is this a perfect solution, certainly not, the fact that the medium of delivery is unsecured (the Internet) makes it questionable. Even if it is delivered via HTTPS and even the application requires the users to connect to a VPN before the users can access the application (this is unlikely), the question remains how can the

server absolutely know that a request is really from an authorize user, the answer is never. Unless there is a way to allow users to provide biometrics information directly to the system (without letting the biometrics information pass on unsecured internet cables, questionable routers and related systems), there is no guarantee. Encryption, decryption technologies and secured application code could help but still hackers have many ways to circumvent security processes so as long as cloud users operate on the cyberspace where cybercriminals operate there is absolutely no guarantee with regards to security. Aside from unsecured medium, there are many other security related questions that cloud computing industry has to answer in order to assure a steady growth and eventually achieve mainstream adoption.

Certainly, cloud providers are seriously working to address all these security concerns and while they maintain that they take security seriously, they will have to be more transparent about it. As businesses migrates more sensitive data and transactions over the cloud, businesses will demand more transparency and security assurances from cloud providers. As cloud becomes more popular, the competition among cloud providers will intensify and as a result, quality of services will improve and the cost will be more competitive. Once the perceptions of businesses on cloud security improved, which means security reports and data breaches incidents show a positive sign, mainstream cloud adoption will follow. If however, cloud providers continue to ignore or fail to address the security concern of cloud users, the trust level of enterprise to cloud based solutions could suffer and as a result of lower trust level, the reverse could happen, de-cloudization [sic] could become the new trend.

In summary, cloud computing is expected to be a significant disruption to business operations and strategies in the foreseeable future. Cloud migration and/or adoption will continue as companies discover and learn more about the many advantages that cloud based services offer. Yet, security issues will continue to be a significant concern for users, aside from application code security, cyberspace security is also going to be a significant problem as enterprise start to migrate more sensitive data and transactions to the cloud. Depending on what is going to happen in the next five years, cloud computing could either achieve mainstream adoption or the reverse, de-cloudization [sic] could start after five years or sooner in case some major security incident happen or a better alternative arises.

5.4 The future of cyberspace security

The majority of the services that are delivered over the Internet are in one way or another handled and/or processed by a server based in the US or in an EU country; hence, any

person could do transactions with EU and the US via these services. Apparently, there is no visa system or border control in the cyberspace, though some countries such as China blocks access to certain online resources, these resources are available to the entire cyberspace community, so Chinese could simply go to Hong Kong to access the banned service. This is what makes the cyberspace a risky place; cyber-criminals could operate anywhere in the world and attack anyone, the authorities seem helpless and couldn't even accurately pinpoint where the crime took place; apparently, IP addresses particularly IPV4 is not a reliable piece of information to point the hackers' location and identity.

As cloud computing's primary platform is the Internet, cloud computing's success also depends on the security of the cyberspace which at the moment not conducive for cloud computing business. However, as cloud adoption continues, the clamor for a more secured cyberspace will grow which will led to a more reliable cyberspace environment.

5.5 Improving Cloud Security

Once the data left a company's server they become part of the cyberspace, the data becomes available to certain authorized cyberspace user/s; hence cyberspace security is important to cloud security. The primary problem of the cloud is, cyber-criminals are all over the cyberspace, so even un-authorized users (determined hackers) could most of the time access other user's data. This means that the security is not just cloud service provider's responsibility, but the entire cyberspace community. Unless cyberspace total reengineering can be done – computer scientist and engineers are now in a better position and more knowledgeable to build a more robust and secure network - we are perhaps far from achieving absolute online security, but there are various steps that the entire community could do now to improve online security and have a relatively safer cyberspace for everyone to do business and hangout with.

5.5.1 Improve Code Security Skills – Software Developers

Software developers have to treat code security as part of non-functional requirements and an essential element of any piece of software they develop. Aside from error handling, software developers should also implement security handling (this is perhaps a useful framework to develop, right now only error handling is explicitly included in programming frameworks). So here are the specific recommendations

- Developers should familiarize themselves on the commonly exploited vulnerabilities (Chapter 4) and create reusable modules and/or functions that they can use on all their projects.

- Software companies/developers should develop an open source Security Framework for the entire programming community to use. A Framework that simplifies the handling of XSS, SQLi, Directory traversal and others mentioned in Chapter 4 will surely help in the development of secured applications.

5.5.2 Provide vulnerability free Web Applications – Cloud Providers

If software providers and developers could deliver high quality and secured application code, hackers will have a hard time to execute their wicked plans and some of them (the mediocre ones) could go out of business soon. Here are the recommendations on how to do this.

- Train developers on secured programming (Chapter 4, section 4.9.5 pages 73-74 vulnerability distribution list shows the security coding skills that a specific programmer needs)

- Implement enterprise security policy strictly; make sure that there is a satisfactory compliance by making it an important part of the developers/software providers' performance metrics.

- Invest on application security audits and testing, by putting a Security QA team separate from the Application Testing Team.

- Have the application tested by third party security provider and be transparent about the results.

- Improve the remediation time; if possible make sure to eliminate serious vulnerabilities in the shortest possible time so not to give hackers enough time to exploit them.

5.5.3 Provide Security Education – Cloud users and Educational Institutions

One of the weakest links in the security system is arguably the system users themselves, particularly the ones who are not privy about the importance of data security and the subject of security in general. This is the reason why social engineering is still a very popular attack vector (Verizon Enterprise, 2013). Regardless how secure a system is, if a user lets a hacker use his/her identity, or help hackers access critical resources there is nothing a firewall or

secured code could do. So cloud users require education here are the recommendations on how to do this.

- Include Security Education in formal studies according to the level of the students Elementary, High School and College. Perhaps, the growing security incidents justify this need (e.g. cyber bullying, malware proliferation via app download)

- Require employees of both government and private employees to undertake relevant security training/seminar necessary to operate securely on the cyberspace.

5.5.4 Establish reliable cloud security rating agencies – Public-Private Institution Joint Initiative

While the so called “Big Three” credit rating agencies - Moody’s, Fitch and S&P- are currently under fire for their highly questionable performance in the past couple of years (the several hundreds of billions of securities that these agencies had given highest rating were downgraded to junk during the 2007-2009 financial crisis) perhaps many will agree that it is still better to have some agencies looking after things, particularly security. At the moment, there are a number of organizations that promotes cloud service transparency one of them is the Cloud Security Alliance, this organization spearheaded a number of initiative such as the STAR or Security, Trust and Assurance Registry; Dave Cullinane, Chairman of the CSA Board of Directors said, “With over 48,000 individual members, and 70 chapters globally, the CSA has become the global authoritative source for trust in the cloud,” (Kari, 2013) major cloud players such as Amazon Web Services, Box.com, HP, Microsoft, Ping Identity, Red Hat, Skyhigh Networks, Symantec and Terremark have submitted themselves before CSA’s STAR program. Although this is a good start, there is still a lot of work to be done, the STAR is a self-assessment based program, the participants answer a questionnaire provided by CSA, the CSA then upload the response of the participant to the questionnaire to their website, without giving it a rating. So here are the recommendations:

- Public and Private Organizations should collaborate to establish appropriately sized, reliable cloud computing rating agencies, just like in the financial sector having 3 agencies to look after cloud security would surely give the cloud computing industry a significant boost.

- Design a clear and transparent rating system where all the enterprise need to do is to know the rating code of a cloud provider to decide which cloud service to use based on price, their actual security needs and the quality of service and the level of security it offers.

5.5.5 Disambiguate Cyberspace

What is cyberspace and what it is not? Who is responsible for maintaining order and security in this space? The growing incident of data breaches justifies the need to have a globally accepted set of rules for using the cyberspace. Here are the recommendations.

- International talks (at the UN level) on Cyberspace should take place. The Security Council (US, France, UK, China and Russia) should agree on a legally binding code on the use of cyberspace which includes clear definition of cyberspace, responsibilities over cybercrimes, how country acts and cooperate on cybercrime investigations.

5.5.6 Cybercrime Response Capabilities

- Countries should setup cybercrime conventions and action centers just like the Convention on Cybercrime of the Council of Europe and the European Cybercrime Centre (EC3)

- Governments around the world should also start developing high tech policing and intelligence capability, not just to protect governments' infrastructure but also to be ready to defend their countries against future cyber terrorists and cyber wars. Hacktivists groups such as Anonymous can easily turn themselves into cyber terrorist group; countries such as China, North Korea, and Iran were accused of organized/government sanctioned cyber-attacks against US and/or allies such as South Korea.

5.6 Limitations

Cloud computing and security is a dynamic topic; things that are related to the topic move quickly such as technology, government issues, best practices, statistics among others. For example, this study commenced in the last quarter of December, as part of the review of related literature an attempt was made to find out whether there is a European agency that handles cybercrime activities and since the European Cybercrime Center (ECE) was not yet established until 1 January 2013, the attempt to gather information and include it in the review failed, it was only in the middle of May when I came across this agency. Similarly, an earlier attempt to find out whether the United Nation has already conducted a comprehensive study about the increasing problem on cybercrime failed, eventually in the middle of June the United Nation's office on drugs and crime published their comprehensive study on cybercrime on their website. The review of related literature and various section in this paper had been revised several time in order to make sure that the latest development in the area of cloud

computing and security is reflected to the final draft; however, due to the fluidity of this subject there is a possibility that some of the figures shown here are no longer the latest by the time it is published.

While all the figures and numbers used in the analysis and other various section of the study are from highly reliable sources, those sources are considered secondary and apparently, everything being equal (size of sample, quality/authority of the respondents, etc.) primary sources are more reliable. Due to time constraint and availability of reliable sources of information/participants, it was not feasible to conduct a survey; however due diligence was conducted in the evaluation of existing sources to be used.

As cloud computing is a massive area, the study was conducted in the context of SaaS, one of the highly subscribed layers of cloud, therefore the discussion such as those related to security as well as recommendations though could also be applied to other layers such as PaaS and SaaS, they are more applicable to SaaS layer.

5.7 Future Research

This study aimed to find out the significant security threats that could potentially impede cloud adoption; as the study focuses on the SaaS layer, the research revolves around revealing the security vulnerabilities of SaaS based solutions. The result of the study is conclusive, technical vulnerabilities do exist; the majority of web applications that are currently online have overwhelming vulnerabilities such as XSS, DS, IL, SQLi, among others. Now that the most commonly exploited vulnerabilities have been revealed, the next logical step is to build a Security Framework API/Package that the software development community can use to handle these vulnerabilities easily. This Framework must be made open source and free for other developers to view and modify to accelerate its development and maximize its benefit to the software development community.

An attempt to expose the identities of the most vulnerable web applications was also made, but since identifying vulnerable SaaS based services is not an essential objective of the study and the information gathered as part of the research are not enough to back the claim, they are excluded in this study. It would be a bold move for future researchers to undertake such a serious subject, a study that seeks to reveal the most vulnerable web applications in the world would definitely draw the attention of the media and may result to more serious discussion about cloud security, particularly if the outcome reveals that MasterCard or PayPal

payment system, have serious vulnerabilities waiting for hackers to be exploited. The result of the study will not just be useful to cloud users, but will also challenge providers to improve the security of their applications; it will also promote transparency in application security. As the only way to prove vulnerabilities is to find and exploit them, the challenge here is to how to go about it, without violating any existing cybercrime law; the act of exploiting Web application's vulnerability is effectively hacking. Perhaps there are exceptions in the law, or maybe the testing could be legally performed in some other countries, this is a serious undertaking but definitely worth the researcher's time.

This study also considered cyberspace security, because cloud (in the context of SaaS) is essentially the cyberspace, a detailed analysis of the cyberspace and cybercrime would also be an interesting topic for future research. A lot of things has changed on the cyberspace in the past decade, from networking technology to software technology; the incoming Web 3.0, IPV6, HTML5, CS3 and of course cloud computing, the cyberspace has definitely become a more exciting place, and an exciting area for future researchers.

References

Books

BUYYA, R., BROBERG, J. and GOSCINSKI, A., 2011. *Cloud computing : principles and paradigms.* Oxford, Wiley-Blackwell.

FURTH, B. and ESCALANTE, A., 2010. *Handbook of cloud computing*. Florida, Springer.

KRUTZ, R. L. and VINES, R. D., 2010. *Cloud security : a comprehensive guide to secure cloud computing.* Indianapolis, Ind., Wiley.

VACCA, J., 2010, *Network and System Security,* Oxford, Elsevier

WINKLER, J. R. 2011., *Securing the cloud : cloud computer security techniques and tactics,* Rockland, Mass. ; London, Syngress.

Conference Proceedings

CHEN, D. and ZHAO, H., 2012. Data Security and Privacy Protection Issues in Cloud Computing. In: Electrical Engineering and Computer Science, *2012 International Conference on Computer Science and Electronics Engineering (ICCEE-2012).* Xi'an, China 27-30 May 2012. Los Alamitos USA: IEEE Computer Society.

HAMDI, M., 2012. Security of Cloud Computing, Storage, and Networking. In: CTS (Collaboration Technologies and Systems), *2012 International Conference on Collaboration Technologies and Systems.* Denver CO, USA 21-25 May 2012. Los Alamitos USA: IEEE Computer Society.

JENSEN, M., SCHWENK, J., GRUSCHKA, N., Lo Iacono, L., 2009, On Technical Security Issues in Cloud Computing. In*: IEEE International Conference on Cloud Computing*. Los Angeles, CA, USA 6-20 July 2009. Los Alamitos USA: IEEE Computer Society.

KULKARNI, G., GAMBHIR, J., PATIL, T. and DONGARE, A., 2012. A Security Aspects in Cloud Computing. In: ICSESS (IEEE International Conference on Software Engineering and Services Science), *2012 IEE 3rd International Conference on Software Engineering and Services Science.* Beijing, China 22-24 June 2012. Los Alamitos USA: IEEE Computer Society.

SABAHI, F., 2011. Security of Cloud Computing, Storage, and Networking. In: ICCSN (IEEE International Conference on Communication Software and Networks), *2011 IEE 3rd International Conference on Communication Software and Networks*. Xi'an, China 27-29 May 2011. Los Alamitos USA: IEEE Computer Society.

SHAIKH, F. and HAIDER, S., 2011. Security Threats in Cloud Computing. In: ICITST (International Conference on Internet Technology and Secured Transactions), *2011 International Conference on Internet Technology and Secured Transactions.* Abu Dhabi, UAE 11-14 Dec 2011. Los Alamitos USA: IEEE Computer Society.

RAMGOVIND, E., 2010. The Management of Security in Cloud Computing. In: ISSA (Information Security for South Africa), *9th International Information Security for South Africa.* Sandton Johannesburg, South Africa 2-4 Aug 2010. Los Alamitos USA: IEEE Computer Society.

Security White Papers

AMAZON, 2013. *Amazon Web Services: Overview of Security Processes* [pdf] Available at: <http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf> [Accessed 1 July 2013].

CISCO SYSTEMS, 2006. *Top Five Security Issues for Small and Medium-Sized Businesses* [pdf] Available at: <http://www.cisco.com/global/EMEA/sitewide_assets/pdfs/you_inc/Top_Five_Security_Issues_for_SMBs.pdf> [Accessed 10 March 2013].

GOOGLE, 2010. *Security Whitepaper: Google Apps Messaging and Collaboration Products* [pdf] Available at: <http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/a/help/intl/en-GB/admins/pdf/ds_gsa_apps_whitepaper_0207.pdf> [Accessed 1 July 2013].

SALESFORCE, 2010. *Secure, private, and trustworthy: enterprise cloud computing with Force.com* [pdf] Available at: <http://www.salesforce.com/assets/pdf/misc/WP_Forcedotcom-Security.pdf> [Accessed 1 July 2013].

Organizational Reports

CDW, 2013. CDW's *2013 State of The Cloud Repor* , [pdf] Illinois, CDW. Available at: <http://www.cdwnewsroom.com/wp-content/uploads/2013/02/CDW_2013_State_of_The_Cloud_Report_021113_FINAL.pdf> [Accessed 10 May 2013].

CLOUD SECURITY ALLIANCE, 2013, *CSA Suvery Results: Government Access to Information.*[online] Cloud Security Alliance Available at:< https://cloudsecurityalliance.org/media/news/survey-by-ieee-and-cloud-security-alliance-details-importance-and-urgency-of-cloud-computing-security-standards/> [Accessed 10 August 2013]

DOE Office of Science, 2007. *Report of the Cyber Security Research Needs for Open Science Workshop* [pdf] Washington, DOE Office of Science. Available at: <http://science.energy.gov/~/media/ascr/pdf/workshopsconferences/docs/Cs_workshop_final_report.pdf> [Accessed 28 March 2013].

GARTNER, 2013. *Gartner Says Worldwide Public Cloud Services Market to Total $131 Billion.* [online] Business Week Available at: <http://www.gartner.com/newsroom/id/2352816> [Accessed 10 January 2013].

GARTNER, 2011. *Gartner Says Worldwide Public Cloud Services Market to Total $131 Billion.* [online] Business Week Available at: <http://www.gartner.com/newsroom/id/1735214> [Accessed 10 January 2013].

IMPERVA, 2012. *Web Application Attack Report* [pdf] California, Imperva. Available at: <http://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed3.pdf> [Accessed 22 June 2013].

IMPERVA, 2011. *Web Application Attack Report* [pdf] California, Imperva. Available at: <https://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed1.pdf> [Accessed 22 June 2013].

INFORMATIONWEEK, 2013. *2013 State of Cloud Computing* [pdf] New York, InformationWeek. Available at: <http://reports.informationweek.com/abstract/5/10475/Cloud-Computing/Research:-2013-State-Of-Cloud-Computing.html> [Accessed 10 May 2013].

KPMG, 2013. *The cloud takes shape Global cloud survey: the implementation challenge.* [online] <http://www.kpmg.com/FR/fr/IssuesAndInsights/ArticlesPublications/Documents/the-cloud-takes-shape.pdf> [Accessed 10 January 2013]

KPMG, 2011. *The Cloud, Changing the Business Ecosystem* [pdf] Available at: <http://www.kpmg.com/IN/en/IssuesAndInsights/ThoughtLeadership/The_Cloud_Changing_the_Business_Ecosystem.pdf> [Accessed 10 January 2013].

PONEMON INSTITUTE, 2012. *Cost of Cyber Crime Study: United States* [pdf] Michigan, Ponemon Institute. Available at: <http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf> [Accessed 4 May 2013].

SANS INSTITUTE, 2007. *Coprorate Espionage 201* [pdf] San Francisco, Maryland. Available at: <http://www.sans.org/reading-room/whitepapers/engineering/corporate-espionage-201-512 > [Accessed 5 May]

SYMANTEC, 2013. *Internet Security Threat Report* [pdf] California, Symantec. Available at: <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf> [Accessed 15 June 2013].

VERACODE, 2013. *Volume 5 State of Software Security Report: The Intractable Problem of Insecure Software* [pdf] Massachusetts, VERACODE. Available at: <https://www.veracode.com/images/pdf/soss/state-of-software-security-report-volume5.pdf> [Accessed 8 June 2013].

VERACODE, 2012. *Volume 4 State of Software Security Report: The Intractable Problem of Insecure Software* [pdf] Massachusetts, VERACODE. Available at:

<https://info.veracode.com/state-of-software-security-report-volume4.html> [Accessed 9 June 2013].

VERACODE, 2011. *Volume 3 State of Software Security Report: The Intractable Problem of Insecure Software* [pdf] Massachusetts, VERACODE. Available at: <http://info.veracode.com/rs/veracode/images/soss-v3.pdf> [Accessed 9 June 2013].

VERIZON ENTERPRISE, 2013. *Data Breach Investigation Report* [pdf] New Jesey, Verizon Enterprise. Available at: <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf> [Accessed 4 May 2013].

VERIZON ENTERPRISE, 2011. *Data Breach Investigation Report* [pdf] New Jesey, Verizon Enterprise. Available at: <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf> [Accessed 4 January 2013].

TRUSTWAVE, 2013. *2013 Global Security Report* [pdf] Chicago, Trustwave. Available at: <http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf> [Accessed 15 June 2013].

WHITEHAT, 2013. *Website Security Statistics Report* [pdf] California, WhiteHat Security. Available at: <https://www.whitehatsec.com/assets/WPstatsReport_052013.pdf> [Accessed 16 June 2013].

WHITEHAT, 2012. *Website Security Statistics Report* [pdf] California, WhiteHat Security. Available at: <https://www.whitehatsec.com/assets/WPstats_summer12_12th.pdf> [Accessed 16 June 2013].

WHITEHAT, 2011. *Website Security Statistics Report* [pdf] California, WhiteHat Security. Available at: <https://www.whitehatsec.com/assets/WPstats_winter11_11th.pdf> [Accessed 16 June 2013].

Online Journal, Magazines and News Articles

AFP, 2012. Sony PS3 Hacked (again): All Future Games Decryptable, No Solution Possible, [online] 7 September. Available at: <http://www.chinapost.com.tw/business/global-markets/2012/09/07/353551/Sony-hit.htm> [Accessed 6 April 2013].

BBC NEWS, 2013. Cyber-attack hits South Korea websites, [online] 25 June. Available at: <http://www.bbc.co.uk/news/world-asia-23042334> [Accessed 3 July 2013].

BLOOMBERG, 2008. *How Cloud Computing Is Changing the World.* [online] Business Week Available at: <http://www.businessweek.com/stories/2008-08-04/how-cloud-computing-is-changing-the-worldbusinessweek-business-news-stock-market-and-financial-advice> [Accessed 10 January 2013].

FOLEY, N., 2012. LinkedIn hack is latest blow to online confidence, [online] 6 June. Available at: <http://usatoday30.usatoday.com/tech/news/story/2012-06-06/linkedin-investigates-security-breach/55423876/1> [Accessed 6 April 2013].

JAPAN TIMES, 2013. Yahoo Japan suspects vast ID theft, [online] 18 May. Available at: <http://www.japantimes.co.jp/news/2013/05/18/national/yahoo-japan-suspects-vast-id-theft/> [Accessed 26 May 2013].

JONES, C., 2013. Twitter says 250,000 accounts have been hacked in security breach, [online] 2 February. Available at: <http://www.reuters.com/article/2013/03/27/net-us-internet-attack-idUSBRE92Q12F20130327> [Accessed 6 April 2013].

KARI, W., 2013. CLOUD SECURITY ALLIANCE FURTHERS GLOBAL TRANSPARENCY EFFORTS TO SERVE ASSOCIATION'S RAPID GROWTH, [online] 23 July. Available at: <https://cloudsecurityalliance.org/media/news/csa-furthers-global-transparency-efforts-to-serve-associations-rapid-growth/> [Accessed 12 August 2013].

KELLY, H., 2013. Apple: We were hacked, too, [online] 19 February. Available at: <http://www.cnn.com/2013/02/19/tech/web/apple-hacked> [Accessed 6 April 2013].

MCAFEE, A., 2011. What Every CEO Needs to Know About the Cloud [pdf] Boston, Harvard Business Review, Available at:<http://hbr.org/2011/11/what-every-ceo-needs-to-know-about-the-cloud/> [Accessed 22 June 2013]

MONACO, J., 2011. *IT Disaster Recovery Near the World Trade Center* [pdf] Louisville, Educause. Available at: <http://net.educause.edu/ir/library/pdf/eqm0144.pdf> [Accessed 15 June 2013].

PEPITONE, J., 2013. 50 million customers hit in LivingSocial hack, [online] 26 April. Available at: <http://money.cnn.com/2013/04/26/technology/security/livingsocial-hack/index.html> [Accessed 27 April 2013].

PERLROTH, N., and HARDY, Q., 2013. Bank Hacking Was the Work of Iranians, Officials Say, [online] 8 January. Available at: < http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0> [Accessed 6 April 2013].

REUTERS, 2013. Microsoft Hacked: Intrusion Was 'Similar' To Apple And Facebook Attacks, [online] 22 February. Available at: <http://www.cnn.com/2013/02/19/tech/web/apple-hacked> [Accessed 6 April 2013].

SANDLE, P., HOLTON, K. and HOLDEN, M., 2013. Internet slowed by cyber-attack on spam blocker, [online] 27 March. Available at: <http://www.reuters.com/article/2013/03/27/net-us-internet-attack-idUSBRE92Q12F20130327> [Accessed 6 April 2013].

SMITH, G., 2013. Facebook Hacked In 'Sophisticated Attack,' Company Reveals, [online] 15 February. Available at: <http://www.huffingtonpost.com/2013/02/15/facebook-employees-laptop_n_2697599.html> [Accessed 6 April 2013].

STRAUSS, 2012. Sony hit by cyber-attack; hackers steal info of its mobile unit clients, [online] 25 October. Available at: <http://www.forbes.com/sites/karstenstrauss/2012/10/25/sony-ps3-hacked-again-all-future-games-decryptable-no-solution-possible/> [Accessed 6 April 2013].

Podcast Lecture and Conferences

DANSEGLIO, 2012, *Ethical Hacking: What Is Directory Traversal?, Ethical Hacking Training* Training [podcast] Fall 2012. Available at: < http://www.trainsignal.com/blog/videos/ethical-hacking-what-is-directory-traversal> [Accessed 27 March 2013].

GANESH, V., 2013. Cross-site Request Forgery (CSRF) Attacks, ECE458 Computer Security. [online] University of Waterloo, Available at: <https://ece.uwaterloo.ca/~vganesh/TEACHING/W2013/ECE458/> [Accessed Date 8 February 2013].

Harvard University Extension School, 2012, *Cloud Computing and Software as a Service, Lecture 1 - (Fall 2012),* CSCI E-175 Lecture [podcast] Fall 2012. Available at: <http://cm.dce.harvard.edu/2013/01/13602/L01/index_H264SingleHighBandwidth-16x9.shtml> [Accessed 12 November 2012].

LEASON, M., ROSE, M. and PASLASKI, S., 2012. XSS / CSRF - DAY 1, CSE825 Computer and Network Security. [online] Michigan State University Available at: <http://www.cse.msu.edu/~cse825/lectures/An%20Idiots%20Guide%20To%20XSS%201.pdf > [Accessed Date 7 February 2013].

KAK, A., 2013. Web Security: PHP Exploits and the SQL Injection Attack, Computer and Network Security. [online] Purdue University Available at: <https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture27.pdf> [Accessed Date 8 February 2013].

Technical Reports

CLARK, D., 2010. Characterizing cyberspace: past, present and future [pdf] Massachusetts, MIT. Available at: <http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf> [Accessed Date 28 March 2013]

KIEZUN, A., GUO, P., JAYARAMAN, K. and ERNST, M., 2008. Automatic Creation of SQL Injection and Cross-Site Scripting Attacks [pdf] Massachusetts, Massachusetts Institute of Technology. Available at: <http://dspace.mit.edu/bitstream/handle/1721.1/42836/MIT-CSAIL-TR-2008-054.pdf?sequence=1> [Accessed Date 8 February 2013]

SKOROBOGATOV, S., 2005. Semi-invasive attacks - A new approach to hardware security analysis [pdf] Cambridge, Cambridge University. Available at: < http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.228.2204&rep=rep1&type=pdf> [Accessed Date 27 March 2013]

ZELLER, W. and FELTEN, W., 2008. Cross-Site Request Forgeries: Exploitation and Prevention [pdf] New Jersey, Berkeley University. Available at: < https://www.eecs.berkeley.edu/~daw/teaching/cs261-f11/reading/csrf.pdf> [Accessed Date 8 February 2013]

Bibliography

Books, Conference Proceedings, Reports and other sources

Alpcan, T. and Basar, T., 2011. *Network Security,* A *Decision and Game-Theoretic Approach.* Cambridge University Press.

Attorney-General's Office, 2013. Cyber-attacks on Australian business more targeted and coordinated, [online] 18 February. Available at: <http://www.attorneygeneral.gov.au/Mediareleases/Pages/2013/First%20quarter/18February2013-CyberattacksonAustralianbusinessmoretargetedandcoordinated.aspx> [Accessed 1 March 2013].

Bisson, S., 2007. *An Introduction to Software as a Service*. London: Faculty of Information Technology ICAEW.

Bleikertz, S., Grob, T., Modersheim, S., 2009, Automated Verification of Virtualized Infrastructures. In*: CCSW 2011: The ACM Cloud Computing Security Workshop.* Chicago, USA 21 October 2011. Chicago, Illinois: Advanced Computing Machinery

Buchanan, W., 2011. *Introduction to Security and Network Forensics.* Boca Rotan FL: CRC Press Taylog & Francis Group.

Chen, Y., Sion, R., Network Security and Applied Cryptography Lab Stony Brook University, 2011, To Cloud Or Not To Cloud? Musings On Costs and Viability. In: SOCC'11: ACM Symposium on Cloud Computing. Cascais, Portugal 27-28 October 2011. Chicago, Illinois: Advanced Computing Machinery

Chu-Carroll, M., 2011, *Code in the Cloud Programming Google App Engine*, Pragmatic Programmers, LLC United States of America

Davidoff, S. and Ham, J., 2012, *Network Forensics tracking hackers through cyberspace,* Pearson Education Inc Massachusetts USA

Forouzan, B.A., 2010. *TCP/IP Protocol Suite. Fourth Edition*. New York: Mc Graw Hill.

Ganssle, J., 2004, *The Firmware Handbook*, Elsevier Burlinon MA 01803 USA

Hwang, K., Fox, G.C. and Dongarra, J. J., 2012. *Distributed and Cloud Computing, From Parallel Processing to the Internet of Things.* Massachusetts: Elsevier

Idziorek, J., Tannian M., Jacobson, D., Department of Electrical and Computer Engineering Iowa State University, 2011, Detecting Fraudulent Use of Cloud Resource. In*: CCSW 2011: The ACM Cloud Computing Security Workshop.* Chicago, USA 21 October 2011. Chicago, Illinois: Advanced Computing Machinery

Kaufman, C., Microsoft Windows Azure Security Architect, 2012 What's Different about Security in a Public Cloud?. In*: CCSW 2011: The ACM Cloud Computing Security Workshop.* Chicago, USA 21 October 2011. Chicago, Illinois: Advanced Computing Machinery

Lam, K., LeBlanc, D. and Smith, B., 2004, *Assessing Network Security,* Microsoft Press Redmond Washington USA

Manferdelli, J., Intel Science and Technology Center for Secure Computing University of California, Berkeley, 2012, Clouds and their Discontents. In*: CCSW 2011: The ACM Cloud Computing Security Workshop.* Chicago, USA 21 October 2011. Chicago, Illinois: Advanced Computing Machinery

Pfleeger, C. and Pfleeger S.L., 2012, *Analyzing Computer Security a threat/vulnerability/countermeasure approach*, Pearson Education Ltd. Michigan USA

Saunders, M., Lewis, P. and Thornhill, A., 2012, *Research Methods for Business Students,* Pearson Education Limited Essex CM20 2JE England

Srinivasan, M., Sarukesi, K., Rodrigues, P., Sai Manoj, P., Revathy, P., 2012. State-of-the-art Cloud Computing Security Taxonomies - A classification of security challenges in the present cloud computing environment*.* In: International Conference on Advances in Computing, Communications and Informatics, 2012 International Conference on Advances in Computing, Communications and Informatics *(ICACCI-2012).* Chennai, India 03-05 August 2012. New York: Advanced Computing Machinery

Stalling, W. and Brown, L., 2012, *Computer Security principles and practice,* Pearson Essex CM20 2JE England

Wang, L., Ranjan, R., Chen, J and Benatallah, B. eds., 2012. *Cloud Computing, Methodology, Systems and Applications.* Florida: CRC Press

Verizon Enterprise, 2012. *Data Breach Investigation Report* [pdf] New Jesey, Verizon Enterprise. Available at: <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf> [Accessed 4 May 2013].

Plymouth University and Kaspersky Lab, 2012, *Cloud Security - Are we high in the clouds? (April 2011),* IT Security for the next generation-International Students Conference-Munich [podcast] April 2011. Available at: <https://itunes.apple.com/ie/podcast/cloud-security-are-we-high/id484989166?i=122263738&mt=2> [Accessed 10 November 2012].

Princeton University, 2008, *Computing in the Cloud - Part 3: "Security and risk in the cloud" (January 2008).* Princeton University Podcast - Computing in the Cloud. Available at: <https://itunes.apple.com/ie/podcast/computing-in-cloud-part-3/id389602908?i=86500311&mt=2> [Accesed 10 November 2012].

Online News and Articles

AFP, The Times. Anonymous' hackers hit Visa, MasterCard and Sarah Palin in WikiLeaks revenge, [online] 9 December. Available at: <http://www.theaustralian.com.au/in-

depth/wikileaks/anonymous-hackers-hit-visa-mastercard-in-wikileaks-revenge/story-fn775xjq-1225968083650> [Accessed 1 December 2012].

BBC News, 2001. US and Chinese hackers trade blows, [online] 1 May. Available at: http://news.bbc.co.uk/2/hi/science/nature/1306591.stm/> [Accessed 1 December 2012].

BLAGDON, J., 2013. Chinese cyberattacks on US traced to this 12-story office building, [online] 18 February. Available at: < http://www.theverge.com/2013/2/18/4003732/chinese-cyber-attacks-on-us-corporations-tied-to-army-base> [Accessed 6 April 2013].

BLUE, V., 2012. PayPal, Symantec hacked as Anonymous begins November 5 hacking spree, [online] 5 November. Available at: <http://www.zdnet.com/paypal-symantec-hacked-as-anonymous-begins-november-5-hacking-spree-7000006876/> [Accessed 1 December 2012].

CHACKSFIELD, M., 2011. CIA website and FBI hacked by LulzSec, [online] 16 June. Available at: < http://www.techradar.com/news/internet/cia-website-and-fbi-hacked-by-lulzsec-966715> [Accessed 1 December 2012].

CHINAHUSH, 2010. Honker Union of China to launch network attacks against Japan is a rumor, [online] 15 September. Available at: < http://www.chinahush.com/2010/09/15/honker-union-of-china-to-launch-network-attack-against-japan-is-a-rumor/> [Accessed 1 December 2012].

COWLEY, S., 2012. An inside view of LulzSec's hacking rampage, [online] 29 February. Available at: <http://money.cnn.com/2012/02/29/htmechnology/cloudflare_lulzsec/index.htm> [Accessed 1 December 2012].

CRIMESIDER, 2010. Scientology Hacked; Church Website Cyber-Attacker Gets Year in Prison for "Anonymous" Invasion, [online] 27 May. Available at: <http://www.cbsnews.com/8301-504083_162-20005928-504083.html> [Accessed 2 December 2012].

DAHONG, M., 2008. The Fifth Attack: on Japanese Websites in 2001, [online] 28 January. Available at: < http://chinascope.org/main/content/view/457/148/1/7/> [Accessed 2 December 2012].

ESECURITYPLANET, 2011. Moody's Hacked, [online] 11 July. Available at: <http://www.esecurityplanet.com/headlines/article.php/3937111/Moodys-Hacked.htm> [Accessed 1 December 2012].

EURONEWS, 2013. Fed downplays hack attack, [online] 2 June 2013. Available at: < http://www.euronews.com/2013/02/06/fed-downplays-hack-attack/> [Accessed 29 June 2013].

FISHER, J., 2012. Anonymous Attacks Vatican For Third Time in One Week, [online] 13 March. Available at: < http://www.webpronews.com/anonymous-attacks-vatican-for-third-time-in-one-week-2012-03> [Accessed 2 December 2012].

FISHER, M., 2013. Hacker group Anonymous is no match for North Korea, [online] 27 June. Available at: <http://www.washingtonpost.com/blogs/worldviews/wp/2013/06/27/hacker-group-anonymous-is-no-match-for-north-korea/ [Accessed 3 July 2013].
GIRIDHAR, 2011. 5 Most Notorious Hacking Groups Of All Time, [online] 26 July. Available at: < http://www.hackdigital.com/5-most-notorious-hacking-groups-of-all-time/ > [Accessed 2 December 2012].

GOLDMAN, J., 2013. Portugal Cyber Army, HighTech Brazil HackTeam Hit Dubai Airport, Hong Kong Police, [online] 22 April. Available at: <http://www.esecurityplanet.com/hackers/portugal-cyber-army-hightech-brazil-hackteam-hit-dubai-airport-hong-kong-police.html> [Accessed 27 April 2013].

GREENBERG, A., 2011. PBS Hacked After Critical WikiLeaks Show, [online] 30 May. Available at: <http://www.forbes.com/sites/andygreenberg/2011/05/30/pbs-hacked-after-critical-wikileaks-show/> [Accessed 1 December 2012].

GROSS, D., 2013. Report: Eastern European gang hacked Apple, Facebook, Twitter, [online] 20 February. Available at: < http://www.cnn.com/2013/02/20/tech/web/hacked-apple-facebook-twitter> [Accessed 1 March 2013].

HITACHI, 2012. List of media coverage on cyber-attacks related to the Senkaku dispute in September 2012 as of October 2nd, [online] 2 October. Available at: <http://www.shield.ne.jp/ssrc/topics/SSRC-ER-12-046-en.html/> [Accessed 2 December 2012].

HUFFINGTONPOST, 2012. Vatican confirms second hacker attack, Anonymous claims responsibility, [online] 7 March. Available at: <http://www.huffingtonpost.com/2012/03/07/anonymous-hacks-vatican-website_n_1327297.html> [Accessed 2 December 2012].

KUMAR, M., 2011. Public Broadcasting Service (PBS) Hacked by Lulzsec, Users data & Database Leaked!, [online] 29 May. Available at: <http://thehackernews.com/2011/05/public-broadcasting-service-pbs-hacked.html> [Accessed 1 December 2012].

LEYDEN, J., 2011. LulzSec hacks US Senate, [online] 14 June. Available at: <http://www.theregister.co.uk/2011/06/14/lulzsec_senate_bethesda_hack/> [Accessed 1 December 2012].

LEYDEN, J., 2011. Portuguese hackers strike back at Moody's downgrade, [online] 8 July. Available at: <http://www.theregister.co.uk/2011/07/08/patriotic_portuguese_hackers_hit_moody/> [Accessed 1 December 2012].

MIRKINSON, J., 2011. Fox.com Hacked By Group Lulz Security, [online] 10 June. Available at: <http://www.huffingtonpost.com/2011/05/10/fox-hacked-by-group-lu_n_860066.html> [Accessed 1 December 2012].

MUNCASTER, P., 2012. Chinese hacktivists launch cyber-attack on Japan, [online] 21 September. Available at:

<http://www.theregister.co.uk/2012/09/21/japan_china_attack_sites_senkaku/> [Accessed 2 December 2012].

NEAL, D., 2012. Sony gets hacked by Anonymous, [online] 6 January. Available at: < http://www.theinquirer.net/inquirer/news/2135722/sony-hacked-anonymous> [Accessed 1 December 2012].

SCHWARTZ, M., 2013. Microsoft Hacked: Joins Apple, Facebook, Twitter, [online] 25 February. Available at: <http://www.informationweek.com/security/attacks/microsoft-hacked-joins-apple-facebook-tw/240149323> [Accessed 1 March 2013].

SELVAN, S., 2013. Dubai International Airport website hacked by Portugal Cyber Army, [online] 20 April. Available at: <http://www.ehackingnews.com/2013/04/dubai-airport-site-hacked.html> [Accessed 6 April 2013].

SMITH, D., 2013. Bank of America Hacked By Anonymous: Hackers Leak 'Secrets' About Executives, Salaries, And Spy Activities, [online] 28 February. Available at: < http://www.ibtimes.com/bank-america-hacked-anonymous-hackers-leak-secrets-about-executives-salaries-spy-activities-1107947> [Accessed 1 March 2013].

TREND MICRO, 2011. *Small Business Is Big Business in Cybercrime* [pdf] California, Trend Micro. Available at: < http://www.trendmicro.com/cloud-content/us/pdfs/internet-safety/tlp_small-business-big-for-cybercrime.pdf> [Accessed 15 June 2013].

THE GURDIAN, 2011. Federal Reserve hacked, [online] 6 February 2013. Available at: <http://www.guardian.co.uk/business/2013/feb/06/federal-reserve-anonymous> [Accessed 16 February 2013].
THE TELEGRAPH, 2011. CIA website hacked by Lulz Security, [online] 16 June. Available at: < http://www.telegraph.co.uk/news/worldnews/northamerica/usa/8578704/CIA-website-hacked-by-Lulz-Security.html/> [Accessed 1 December 2012].

THE TELEGRAPH, 2009. Top 10 most famous hackers, [online] 27 November. Available at: <http://www.telegraph.co.uk/technology/6670127/Top-10-most-famous-hackers.html> [Accessed 2 December 2012].

TIMESOFHACKER, 2013. Hong Kong Police Hacked by Portugal Cyber Army, [online] 22 April. Available at: < http://www.timesofhacker.com/2013/04/hong-kong-police-hacked-by-portugal-cyber-army.html> [Accessed 27 April 2013].

W3B Security, 2013. Hong Kong Police site hacked, 45 credentials leaked, [online] 10 May. Available at: <http://www.w3bsecurity.com/hong-kong-police-site-hacked/> [Accessed 26 May 2013].

WEISENTHAL, J., 2011. Resurgent LulzSec Attacks Government Sites In Portugal, [online] 8 December. Available at: < http://www.businessinsider.com/did-moodys-website-just-get-hacked-by-someone-angry-over-portugal-2011-7> [Accessed 1 December 2012].

WILLAN, P., 2012. Vatican confirms second hacker attack, Anonymous claims responsibility, [online] 13 March. Available at:

<http://www.computerworld.com/s/article/9225159/Vatican_confirms_second_hacker_attack_Anonymous_claims_responsibility> [Accessed 2 December 2012].

WILSON, T., 2011. Did Moody's Website Just Get Hacked By Someone Angry Over Portugal?, [online] 7 July. Available at: <http://www.darkreading.com/attacks-breaches/resurgent-lulzsec-attacks-government-sit/232300133> [Accessed 1 December 2012].

WILSON, T., 2011. Resurgent LulzSec Attacks Government Sites In Portugal [online] 8 December. Available at: < http://www.darkreading.com/attacks-breaches/resurgent-lulzsec-attacks-government-sit/232300133> [Accessed 1 December 2012].