Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Cloud Computing - Maze in the Haze

When Amazon announced its EC2 environment in August 2006, one might not have imagined the change in trend this event would bring into the IT industry. With far more competitors to Amazon, one cannot help but admit to the fact that cloud computing will be a major catalyst for an evolution in the way the industry works. The cloud traverses international borders, taking our data with it and leaves us with a trail of concerns about data access, security and availability. After all these years, the question remains Are we ...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

Cloud Computing – Maze in the Haze

GIAC (GSEC) Gold Certification

Author: Iyengar, Godha Bapuji., Godha.iyengar@yahoo.com

Advisor: Westbrock, Marc

Accepted: October 17, 2011

Abstract

When Amazon announced its EC2 environment in August 2006, one might not have imagined the change in trend this event would bring into the IT industry. With far more competitors to Amazon, one cannot help but admit to the fact that cloud computing will be a major catalyst for an evolution in the way the industry works. The cloud traverses international borders, taking our data with it and leaves us with a trail of concerns about data access, security and availability. After all these years, the question remains "Are we ready to move our data to the clouds?" This paper throws some light on certain differences in a few laws from India, USA and UK that indirectly or directly affect the way clouds work, what it entails to stay compliant and why it might be a good idea to invest in a team of security advisors fortified with a team of legal experts.

© 2011 SANS Institute, Author retains full rights.

1. Introduction

In recent days, "Cloud Computing" has become a great topic of debate in the IT field. Clouds, like solar panels, appear intriguingly simple at first but the details turn out to be more complex than simple pictures and schematics suggest. Simply put, the Cloud is just the mobile and remote data center that you share with your neighbors and strangers alike. Think about a school or a church renting out their extra space for Sunday schools or parties. It is easy and seems cost-effective at first but has its own issues. There are no decorations, no clean-up, no customizations, restrictions based on site, and many other inconveniences, but do we go for it? It all depends on what our priority is; if we want a cozy family party with 1-1 face time with everybody and a nice environment to relax, the home is the way to go. Or go the church way if you are ready to accept some limitations to get out of the hassle of cooking, cleaning, changing your sheets, your curtains and your garbage bin liners.

There is no dearth of resources on the internet about the cloud in general. The best place to start off would be the NIST's definition on clouds, their standards roadmap and the reference architecture. See (Mell & Grance, 2011), (Hogan, Liu, Sokol & Tong, 2011), (Liu, Tong, Mao, Bohn, Messina, Badger & Leaf, 2011).

This paper will mention some of the laws pertaining to Information Technology (IT) and Information Systems (IS) from the countries that the author has lived and worked in namely, India, the United States and United Kingdom. It will also study how or why our ways and the laws might have to be inspected, enhanced, empowered or simply re-framed to be able to support this shiny new futuristic computing.

Disclaimer:

The views presented here are merely the author's own and have been evaluated against various documentations available globally in various online forms, and through extensive research and discussions with various subject matter experts. No part of the document should be taken "as-is" or as substitute for expert legal counsel. Moreover, it is to be kept in mind that cloud computing is still an evolving topic and the contents in this paper are only true at the time of this writing. Hence the readers are advised to consult

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

current information for update on any specific topic. Neither the author, nor the contributing experts or SANS for that matter, take any responsibility for any actions or results thereof, taken on the sheer basis of this document. Please consult your legal team before making any critical decisions pertaining to your business, using this document ONLY as a reference.

2. The Landscape of IT and related laws across India, US and UK.

To begin with, fundamental changes in computer architecture and increases in network capacity are encouraging software developers to take new approaches to computer-science problem solving. The rapidly changing economies of the world and the fact paced life style are all contributing factors for new improved ways of doing things and computing is no different. In an effort to cut costs, experts are always on the lookout for better ways of doing things and with more and more people using the Internet, the boundaries of the countries seem to be shrinking by the day. According to the Internet Statistics Compendium, there are more than 2 billion internet users worldwide. 39.8 percent are from Asia-Pacific, 27.6 percent from Europe, and 15.9 percent are from North America (Econsultancy, 2011). Although the internet penetration rate in Asia is a mere 23.8 percent, according to the InternetWorldStats.com, it still accounts for the most internet users in the world (Internet World Stats, 2011). Cloud computing enables e-retailers to market and sell their goods more efficiently across the regions. Small and medium enterprises now do not need to own huge infrastructure to provide quality shopping experience to the consumers. Cloud computing also enables them to provide stable and quicker services a fraction of the cost.

Looking back at what is already been in place, after all these years, now more than ever business critical applications have to not only work for the end user but also provide secure and reliable solutions which comply with both general regulations of IT governance and business specific regulations.

Some of the general regulations that need to be met include SAS 70 which refers to "Statement on Auditing Standards 70: Service Organizations," issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) and

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

the Payment Card Industry's Data Security Standards (PCI DSS). The Federal Information Security Management Act of 2002 (FISMA) is a US federal law set in place to ensure adequate control for security and network around their operations and assets. A lot of monitoring data is collected as a part of this act and it is to ensure adequate measures exist to protect the Information technology and Information systems assets. In UK, HMG ICT systems follow a similar compliance based on CESG's Good Practice Guide no.13 (GPG 13.). The Gramm-Leach-Bliley Act (GLBA), also known as The Financial Modernization Act of 1999, was enacted to ensure protection over customer's records and information.

So even though these standards and regulations have been in existence for quite some time, the advent of cloud computing opens up yet another dimension to the picture of information resources. Trade and commerce over the internet not only worry about their local jurisdiction within which they transact but also about trans-border data flow across the globe.

2.1. India

India is the second largest country in terms of world human population next to China and she is also the most competitive one in today's global IT market. It also has the fourth largest economy as per purchasing power parity statistics. With this background in mind, it is very easy to assume that cloud computing might be riding high in India already. Far from truth, this statement only adds to the doubts and concerns, organizations outside India have developed. While it is true that some of India's critical infrastructural aspects including basic needs such as food, clothing, health, hygiene and education are still a luxury for many rural areas, it can by no means be generalized to the entire country. The large cosmopolitan and metropolitan cities of India are the highest producers of talented, educated and most ambitious of the IT workers. Yet, in these so-called posh cities lie the very dirt and grime of the city in whom the heart of the city beats, longing for a piece of bread of the day or a sheet of tin over their heads for a roof and a yard of cloth to cover the dignity. There are these people who might not even know what an Internet Explorer is or what the cloud is. The only cloud they know is the one

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

that brings rains and consequently many troubles with it. Such is the diversity of this land.

In spite of various media reports now and then, India still seems to be the top IT services provider due to reasons such as low cost labor, availability of well educated, good English-speaking personnel and the government's willingness to comply with parent company's laws along with its country's governing laws (SourcingLine, 2011).

2.1.1. The Indian IT Landscape

Just because Indian companies are well versed with outsourcing and providing services, it cannot be assumed that they are all ready to provide cloud-based services. It is very important to carefully assess the business goals, short-term and long-term plans and evaluate it against the vast backdrop of Indian landscape in its true sense.

India still has its Panchayat System (India's rural self-government system) namely gram panchayats/Zilla Parishads. Refer to the 73rd Amendment, Constitutional Act 1992 (National Informatics Center, 2011) which provides constitutional status to many such institutions of self-governments. It is a very important factor to be considered because all states excluding but a few have the self-governance system in place and per constitution they have a right to partake in the development of their area. This may not pose a problem in general but hierarchy and bureaucracy matter. By the time an issue reaches the right hands it may get drastically distorted or disproportioned – that is if it manages to reach the right person at the right time? Sometimes it might never even end up being heard. Think about this when something goes wrong and you are waiting to get justice, sometimes in all reality of the circumstances, you are still waiting. While there are organizations striving to provide a neutral ground to fight our battles on, such as the most recent Jan Lokpal Bill (India Against Corruption, 2011) or the Anti-Corruption Bill, we cannot ignore the fact that trying to pass through hoops for a solution or for justice does not generally scale well in terms of time and money.

We need to do our homework, and have to get everything down in the contract. Spell out the do's and don'ts and what happens if not. No matter which land, laws of every land have something in common, employ a legal team to decipher the jargon and use their services more than ever now and involve them right in the initial phases of

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

discussion with the cloud providers to better understand their body language and their "fine prints". Employ a local team of lawyers who would work hand in glove with the onsite legal team. Let them do the drafting for you. A couple of visits back and forth might be a very good idea as an investment. Security folks and lawyers have typically been viewed as a hindrance to a project effort, but with the clouds coming in, they are the people to go to first! (Overby, 2011). Organizations such as National Association of Software and Service Companies or NASSCOM, provide a lot of support to software trading. Laws which affect outsourcing such as Tax laws, Import/Export Laws, Investment Laws, Indian IT Act 2000, Indian Copyright Act 2000 which covers Intellectual Property Rights, ("Intellectual Property Rights", GOI) and the Product Patent Act 2005 are but a few examples which a country's government has to create in order to provide high quality services to the outsourcing clients. Irrespective of many such measures, things happen, and relationships break damaging trust and business ties abruptly between the two entities (Chapman, 2009). Given this landscape, how are the laws being modified to accommodate even more volatile structure? Come to think of it, this can give nightmares to the analysts today. For example, we all know the Blackberry issues (Whittaker, 2010), that took form in various countries in the Middle East and South East Asia. India was also one of the countries that wanted control over Blackberry data. According to its policies any encryption software over the limit of 40-bit encryption level is not permitted and providers of such technology beyond the stated limit must seek explicit permission from the government and handover the decryption keys to the government in the interest of national safety. While the Indian government is still holding on to its 40-bit encryption level (Singh, 2010), United Kingdom and the United States both have far more defined encryption and cryptography export policies and a stronger key strength. Consider this when evaluating business impact levels for customer data., since when encrypted data in the cloud traverses this region it will either have to be reduced to conform to their policy, or the decryption keys handed over to the government officials. This factor can become one of the concerns of cloud computing if governments across borders do not work towards a common and globally applicable solution.

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

Apart from thinking about laws, there are other factors that need attention. For example, it might be very natural for us to expect a Data Protection/Data Privacy Notice displayed or maintained in a file in a photography studio in UK/EU and the US but not so usual in a studio in India. Also, piracy is a big problem in India, like many other countries around the world. While there are international laws on preventing piracy and copyright infringements, they are not so well implemented across the general public in India.

Consider this example: Xerox or photocopying centers are a common sight in the Indian commercial setting, averaging 2-3 within a walking distance. They are mostly funded by government grants or self-employment grants and cater to the needs of the local public for various reasons such as simple bills to forms and school or college textbooks or exam guides or past exam model papers borrowed from friends or libraries. . The average education level of the proprietor is just about enough to qualify him/her for the grant. These shops or their owners have no idea of copyright laws or Intellectual Property laws and people who use the services do not consider taking a copy of something as infringing upon some copyrights (Nair, Barman & Chattopadhyay, 1999). On a side note, it is important to observe that the Indian legal system has always been striving to be a strong competitor and a well informed neighbor by being involved in the UN as a forming member, and various other organizations such as the World Intellectual Property Organization (WIPO). But question remains as to how many of its citizens actually are aware of these facts and realize the value of the laws, treaties and associations?

Awareness about internet privacy, copyright infringements, data privacy and Information Systems security in general public is at a low rate and you cannot expect such crowd to understand highly convoluted IT laws with a lot left to legal intellectual interpretation. These are the places where government needs to raise the overall standard of security. Mere existence of laws does not guarantee safety. It is very important for the laws to be accessible to the common man and for the laws be written in such a way that the common man can interpret it without ambiguity. Considering India's population density, literacy rates, and its demography this is one of the most challenging aspects of Information Security, Data Protection and Privacy in India. We are talking about the shopkeeper or the hawker who has no idea whatsoever about these laws and his/her

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

rights; while at the same time, has children who might unknowingly be the victims of internet scams and offences through their hi-tech friends.

Schools, colleges, libraries and community services must be elevated to a level where everyone gets equal opportunity to learn and be aware of their socio-political issues. Democracy is good only when it is in the hands of well aware public. Governments should strive to bring this awareness into the common man's reach and not just to the children of the IT workforce.

While Indian network is still evolving, there is still the question of the internet reaching every household in India. According to this independent website statistics ("Internet usage stats," 2011) India's internet penetration stands at 8.4 % for its entire population whereas China stands at 36.8%. The literacy rate in India is still struggling at around 64.84%, with a big gap between male and female literacy rates (National Informatics Centre, 2010). Illiteracy, poverty, proper hygiene, basic and higher education opportunities, gender disparity, income disparity although not directly related but are impediments to its growth. One can see quite a contrast in its willingness to become a super power and the lack of basic education and hygiene in the vast rural areas of the country and its overpopulated cities struggling to provide a stable internet bandwidth to homes against a trove of scams/scandals.

Frequent power outages due to electricity shortages, electricity losses during transmission and distribution (Tiwari, 2011), and electricity thefts are major problems related to electricity supply. You may be thinking how this would affect the clouds – but think again, electricity is the juice to the internet! So availability and reliability becomes a major factor. Do not overlook these factors when considering a cloud from the region. Ask about their business continuity and disaster recovery plans and make sure to check their electricity supplies. So when a cloud provider promises 100% or even 99% uptime and availability, it is advisable to check the fine print and this applies to cloud providers from any region.

While many of India's laws are based on the model law and the British legal system, it should be interesting to note that it lacks any central Data Retention or Destruction laws. While there are local agencies which create their own requirements for

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

retaining records, by no means is this the norm for the internet community. Also, no specific laws or regulations on CCTV's or their usage were found online so while everyone in the country is free to install CCTV's, there is no guidance on how the data should or should not be used and the legalities involved.

It is to be noted that the IT Act 2000 of India did have some text about infringing privacy (CRID, 2005), but the recent amendments to the act in 2008 (Sandfiorenzo, 2011) have evoked greater debates on how it dilutes the already weak IT Act of 2000 and vests power in the hands of security agencies thus violating fundamental human rights of the people. This is a very important point to be considered when working with cloud providers from the region.

2.2. USA

The US has always remained one of the most migrated countries according to one of the immigration statistics (Esipova, Ray & Srinivasan, 2010). The land of opportunities as it is called, gives these people a chance to live the "American Dream" albeit with a few challenges.

United States is probably the most litigated country with laws for everything. if we look at the laws enacted by the US, one cannot help but wonder is there anything that "they" haven't covered? What makes it even better is that the common man has access to the law and has the right to express or exercise his rights. What makes it worse is that often the same common man exploits these privileges given to him by his country's constitution making the laws seem like a "shot-in-your-own-foot".

While it would be unfair to expect the rest of the world to have similar laws to the US, it would be equally unfair to the law-abiding citizens of any country who unwittingly become victims of incidents brought on by unscrupulous citizens of other countries with fewer IT/Security laws and weaker legal system. The best way is to find a balance between "their" laws and "our" laws and devise a common platform on the basis of which offending criminals can be prosecuted.

For example consider the Digital Millennium Copyright Act (DMCA). It prohibits any circumvention of technological measures of data and copyright protection of works

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

without the permission of the authors or the law. It can also apply to attempts of decryption of encrypted data or descrambling, removing or by any means bypassing the security measures in place. Yet liabilities of infringement are taken care of separately under the Copyright Act. See this link in the footnotes for the Copyright Law in its entirety[1]. Another law that is supposed to keep computer hackers at bay is the Computer Fraud and Abuse Act, which imposes penalties to any act of unauthorized use of a protected computer or impairment of integrity of the system. Title 18, Chapter 47, Sec 1030 deals with fraud and related activities in connection with computers and is applicable to "any" person as defined under e (12). The USA PATRIOT Act 2001 makes a clear distinction between United States citizen and a non-Citizen and their handling within the jurisdiction of the country. It clearly explains in the act what a non-citizen can expect if he/she partakes in any criminal activity. For more details on the act please refer to the footnote link[2]

The Electronic Communications Privacy Act (ECPA) restricts the interception of electronic communications and prohibits access to stored data without the consent of the user or the communication service. Consider the conflicting act under the Electronic Discovery in the Federal Rules of Civil Procedure –the e-Discovery act states that businesses must be quickly able to find data when requested by law in litigations. While the ECPA restricts access to data under the Stored Communications Act (SCA), it is very important to discuss data e-discovery and recovery options with your cloud provider when planning storage and backup needs. We observe that these acts have now to be at least modified to reflect the right terminology with respect to international movement of data and with specific explanation of generic and vague terms such as "provider", "user" and demarcate the limit of the law in clear and simple words (Kerr, 2004).

One such important development in the world of internet was the introduction of the Consumer Internet Privacy Protection Act of 1999. It states that "the service shall not disclose to a third party any personally identifiable information provided by a subscriber without the subscriber's prior informed written consent". Under Sec 4 of the act, the definitions, "the term third party" can mean a person or other entity other than the service or its employee or the subscriber to such service. While the scope seems broad enough to cover any one under the US Law, it does not clearly state how it would treat international

© 2011 SANS Institute, Author retains full rights.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

third parties. An important aspect to this law is the Freedom of Information Act (FOIA) which gives right to information to citizens as well as non-citizens! It is not completely clear as to how non-citizens would be prosecuted. This clarity is very important keeping cloud computing in mind.

More on the FOIA: In the US, this act allows third party access to personal information under strict terms[3] (See page 14 under section 4). Comparing this with the UK's Freedom of Information Act 2000 (FOIA); the UK law clearly states that under no circumstances can the personal information be requested under this act. All such requests are dealt with separately as Subject Access Request under the Data Protection Act. Personal Data is exempt under sections 40(1) and (5) ("Freedom of information," UK). India's Right to Information act grants this privilege only to its citizens or to a third party organization with some restrictions, see Chapter II, section 8) of this footnote link [4]. A simple review of related laws across the three countries gives a lot of insight into why and how is it important to have well-written contracts with cloud providers from these regions. See this well written document by a French law firm in the footnote [5].

Consider another aspect of trade, Cryptography. The Federal Register Vol 75. No. 122, has information on encryption and its export controls. The document also states that "Export controls work best when all countries implement the same export controls in a timely manner". Reading the document further under Part 740, reveals that the Bureau of Industry and Security does not require reporting exports of encryption commodities with symmetric key length not exceeding 64-bits.

The Wassenaar Arrangement helps countries provide a common ground for exports. If you are encrypting your data in transit and exporting it, it is strongly recommended that you review the following sources for information on why cryptography is export controlled (from RSA Labs) [6] and which countries are members of the Wassenaar arrangements in this link. See footnote[7].

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

2.3. UK/EU

With its rich history, beautiful landscapes, wonderful architecture and an envious transport system, the European continent has always been ahead of its time and paving way for many other countries.

1926 saw a major development in Britain's history. This is a year that probably changed everything by just one act - The Electricity Act of 1926. See this timeline document from the Museum of Science and Industry's collection centre for a great overview on electricity and its evolution in Britain in footnote[8]. The Electricity Supply act proposed integrating UK electricity through a centralized national grid which will power electricity to be used by everyone in the nation. Centralizing electricity not only improved economies of nation but also transformed lives in every way from simple light bulbs to the incubators striving to keep a life alive in a neonatal unit. Life would have struck a totally different note on just coils and dynamos. There must have been resistance in the 1920-30's when people wanted to move energy production to a central location rather than in ones basement. There may have been protests over those ungainly electric structures hovering over beautiful landscapes literally 'ruining' the views. Nevertheless, people grew out of it - people grew into it. The Grids as they all came to be known, gained their entry into a common man's picture window. Who knows, if the grid was never made, may be there wouldn't have been the internet - there wouldn't have been the 'Cloud'.

Doing business with EU and UK can be a bit challenging because of very strict EU privacy laws[9]. Due to the government mandates, it is no surprise if one has to be security cleared twice in the same council (area) just to volunteer for two separate institutions. For many jobs, one has to be at least 3 years resident of UK/EU and have any of these - Counter-Terrorist Check (CTC), Baseline Check (BC), Security Check (SC), and Developed Vetting (DV) or a Communications-Electronics Security Group (CESG), Listed Adviser Scheme (CLAS) already approved, these can take anywhere between 15 days to 6 months and can cost thousands of pounds for companies to have it done on the person. For more details on what these acronyms mean please refer to the link in the footnote [10].

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

More on the processes: Here in the UK, one has to order prescription refill, either personally at the clinic through a written request or send in an email to the nurse requesting for one with clear instructions. Then pick it up from the clinic and give it to the pharmacy. As a contrast, in the US, one would call up the nurse for a prescription refill, they would check the records, validate the person and if they were due for follow-up tests before a refill – they let the person know, they would also verify if the insurance or their pharmacy had changed. One can simply go pick the prescription up without even getting out of the car using the world-famous "drive thru" concept. This was an example to how different countries have different way of doing things; it is this difference that goes a long way in explaining why it is important to be well informed and always have a subject matter expert at hand, be it security or legal.

Consider another example here of that of photographers. Photography laws are vague on this side of the pond. For instance, it would be considered invasion of privacy if a photographer takes a picture of his own daughter or son at a football match but includes other team members without the explicit consent of their parents. See these links for UK[11] and for the US[12]. In the UK, photography in a public place also needs to be done with care and sometimes subject to consent from the people involved, especially children due to the Protection of Children Act 1999. On the contrary in the US, once a person is in a public place, his/her privacy rights won't matter unless he/she explicitly expresses to be left alone. "The reason that privacy laws in Europe and the U.S. are so different springs from a basic divergence in attitude: Europeans reserve their deepest distrust for corporations, while Americans are far more concerned about their government invading their privacy", says Bob Sullivan in this article on MSNBC (Sullivan, 2006). In India there are certain restrictions on ariel shots such as in defense areas but these laws have been relaxed to some extent in the recent past. People are now allowed ariel photography from aircrafts in flight. But a lot needs to improve in India in this area as a general feel among photographers there is that the laws are too vague, tight and sometimes pointless (Bhuta, 2010). We are all living in a world, age and countries where we are paranoid about everything around us and have laws about simple things that might have been perfectly normal 10 years ago.

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

We have also read earlier in this document that India does not have a central data destruction policy, consider in contrast countries like UK which have to conform to HMG Infosec Standard 5 and have regulations that govern various aspects of data erasure and disposal.

- Data Protection Act
- Environment Act
- WEEE Directive
- Hazardous Waste Regulations
- Landfill Regulations
- Electrical Equipment (Safety Regulations)
- Basal Convention, Trans Frontier Shipment of Waste
- Sarbanes-Oxley Act
- Sale of Goods Act
- Distance Selling Regulations

The most common law that directs most of the data disposal/erasure methods is the HMG IS5 Data Sanitization Method. The Infosec Standard 5 states this:

MANDATORY REQUIREMENT 45
Departments and Agencies must ensure that all media used for storing or processing protectively marked or otherwise sensitive information must be disposed of or sanitised in accordance with HMG IA Standard No. an 5 – Secure Sanitisation of Protectively Marked or Sensitive Information ("HMG security policy," 2008).

Looking at the data handling procedures across continents one cannot help but think about how serious data destruction is in some countries in contrast to others who do not have proper data destruction rules/laws to start with. Awareness of data destruction and disposal laws of various regions important factor in cloud computing.

UK's department of education recently released a press note dated 11 July, 2011 announcing some changes to one of its laws, a no-touch policy in schools. The revamped law has been condensed from voluminous 600 pages of guidance to merely 52 pages (DOE, 2011). This example does not directly relate to cloud computing, It relates to

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

education laws but it does exemplify how each country differs in its remediation, adoption and implementation of various issues at hand. It goes a long way to show that it is no easy game to work in the EU/UK regions - with such close control on privacy laws, cloud computing seems to add another layer to complexity.

In order to do business with EU/UK companies other countries have to conform to these strict guidelines and mandates otherwise you simply miss out on the business. The US-EU Safe Harbor agreement was an intelligent way to find a common ground to work upon A similar pact was signed in 1993 and later revised in 2008 in The Swiss Federal Act on Data Protection (FADP) too. Organizations can self-certify themselves with an approved fee if they are to deal with personal data from Switzerland or European Union nation. There is also an annual reaffirmation of your organization's conformity to EU or Swiss Safe Harbor principles. If you don't conform, you are simply denied access or in other cases enforcement action is carried out by the authority. See the EU Directive here in this footnote link[13].

While EU and its nations follow a strict exclusion policy for security, in all practical terms this is the very reason for cloud computing being a bit slow on the adoption here. Companies are hesitant to accept a novel idea and the immature technology. They are reluctant to vest their interests and their trust in cloud providers from other "inadequately protected" regions.

3. Outsourcing, Cloud sourcing or Do-It-Yourself?

A wealth of articles can be found which talk about Cloud Computing and to be or not to be. Per se, cloud computing is no different than the application service providers or ASP as they are commonly known, in the 90's or Outsourcing in the 2000's. Technologies have evolved since then and companies which were either entombed in the dot-com era or which managed to survive have significantly contributed to today's Cloud era. Keeping this in mind, the services offered by the cloud are only akin to what wireless does to a traditional network – i.e., provides more flexibility, amidst a whole new range of security problems and risks.

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

As in the case of outsourcing, with cloud sourcing it is very important to clearly define business goals, and set limitations on what goes out. You also must take care in drafting and reviewing business proposals and contracts to ensure every foreseeable risk has been accounted for. Then again, as in the case of outsourcing, one would also place their trust in the 3rd party with which the company is going to work with. Where outsourcing differs from cloud is in the physics of the services. In outsourcing, we know the data X resides in a location Y with a 3rd party Z. Hence it is quite easy for our legal team to draft a contract keeping in mind the jurisdiction of the location Y. It would then make it easy for the auditors to carry out their checks based upon what's in the contract vs. what's visible; any variable is remedied or litigated based on the criticality. All rules, laws, frameworks have been written with this physics in mind which cloud computing now seems to defy.

4. Legal Weds Technology

Cloud Computing raises as many eyebrows as it frowns lips. While many major organizations have contributed to its popularity, adoption of a revolutionary way of working has been slow. This can be mostly attributed to the human tendency to not accept 'change'. Usually it is slow and quite challenging.

4.1. Cloud and the Legalities

The subject matter of cloud means a lot to the IT community and it means even more to the legal community today. Organizations and enterprises adopting the strategies of cloud only realize that they should be willing to go through the 'growing pains' that we all have experienced as a child during our growth spurts and today we probably don't even remember there was such a thing as 'growing pains'. Just like the modern electricity led to the advancements of not just the electric sector but growth in every aspect of human life, cloud computing undoubtedly is giving rise to new roles, new designations, new devices, new techniques of management, new ways of working, new infrastructure, new educational avenues for schools, colleges and universities, and finally new cyber crimes, new laws, new penalties and new issues for the legal community.

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

Lawyers are in demand more than ever to ensure the sanity and validity of the contracts and to help the common man (a.k.a. the businesses) to interpret and understand the legalese of these contracts. Lawyers help not only in drawing lines for businesses on the cloud but also help erase offending lines or in cases where lines have been crossed, help bring justice to parties involved.

They are now in the forefront of contracts since it is all the more important to be clear and precise in defining business boundaries and terms, in black and white, before any financial or infrastructural relationships are established between the cloud services provider and the business entity. It is wise to employ a team of legal experts who are well versed with "clouds" early to help you formulate the right contract with the cloud providers, rather than to employ them at the later stage for fighting of injustice. But with the relative novelty of the concept of cloud computing the legal community also has to learn through the school of hard knocks and has to go through the 'growing pains'.

Just like the electricity law changed the lifestyle of people and brought in new trade and commerce, people and their lives were never the same again. New opportunities came up every day and with it came new way of doing things and learning things. Due to sheer flexibility it offers and also due to the fact that resources are now more globally accessible than ever before, cloud computing will give rise to the percentage of mobile workers. Employees can have more flexibility in their working conditions ranging from home offices to cafes to beaches. This calls for eased export, trade and labor laws. As more and more data will be available externally through the web, work from anywhere takes on a new meaning.

There have been restrictions on what we could do remotely mainly due to the enterprise's unwillingness to "open-up" or broaden their network boundaries and legal factors governing the businesses, technologies and security. For example, if a full time security analyst migrates to another part of the world, he or she cannot take the work with them today due to nature of the work and "legal reasons" surrounding it. This scenario has to change as more and more data moves to the clouds. The export, trade, commerce, labor telecommunications and network laws have to be reviewed.

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

Consider another apparent success point of the clouds: Since there is minimal capital expenditure, any small and medium business (SMB) entity can easily boast of great technical infrastructure without much ado on their part. This also means that dismantling will be easy, which means there is a substantial business risk in working with partner companies.

For example, on an average, it takes about 25 GBP in the UK to setup a limited company legally (companies House, 2011). All you need is a registered office, which can be provided by well recognized and authorized third party vendors. So, investments have to be made very carefully, keeping in mind the history of the company, its credentials and strong legal bindings.

It's easy for any person to incorporate a company overnight and dissolve a company - since it's quite easy with cloud computing to establish critical resources. More than ever, now the company laws have to be stronger, the trade laws have to be stronger. Many small companies will boast of "great" resources, but might cut short in their terms with the cloud vendors and in the process might prove very risky to do business with. So check and re-check the terms and conditions of the contract and make sure to define resources and their levels of importance to the organization. The contract should clearly demarcate lines of control over resources.

Cloud computing will also give rise to a new generation of legal designations, Security designations, and a whole new slew of cloud software application developers, designers, architects, data managers, network engineers etc.,

Gearing up for the legal aspects that the world of cloud computing brings is also a major part both providers and subscribers of the cloud. On Jan 20th, 2010 Brad Smith, senior vice president and general counsel at Microsoft Corp., urged both Congress and the information technology industry to act to ensure that the burgeoning era of cloud computing is guided by an international commitment to privacy, security and transparency for consumers, businesses and government. Mr. Smith shared the results of a survey completed by Microsoft. The survey found that while 58 percent of the general population and 86 percent of senior business leaders are excited about the potential of cloud computing, more than 90 percent of these same people are concerned about the

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

security, access and privacy of their own data in the cloud. In addition, the survey found that the majority of all audiences believe the U.S. government should establish laws, rules and policies for cloud computing (MS Press Release, 2010).

The Centre for Commercial Law Studies (CCLS) at Queen Mary, University of London in collaboration with Microsoft initiated the QMUL Cloud Legal project to undertake academic research in relation to cloud computing and to disseminate the key findings of that research. According to their website the purpose of this project is to reduce that uncertainty via the production and dissemination of a series of scholarly yet practical research papers to address various legal and regulatory issues that will be fundamental to the successful development of cloud computing. It is intended that the research papers will demonstrate thought leadership in several complex and difficult areas of law and regulation that are of vital importance to governments and businesses globally. This initiative aims at delivering a series of scholarly yet accessible papers covering important legal topics such as Cloud computing contracts, Data Ownership and Proprietary Rights in the cloud, Data Protection Law in the cloud, Interoperability and Antitrust issues, Cloud Governance and other related topics (Webmaster, QMUL).

Similarly a major law firm in the UK, JISC Legal has responded to a growing demand for guidance on cloud solutions by creating a comprehensive 'Cloud computing and the law' toolkit. According to their website, the aim of this resource is to guide educational professionals through the legal aspects of implementing cloud computing solutions in their institutions (JISC, 2011).

The publications in the toolkit are:

1. Report on cloud computing and the law for UK further and higher education
2. User guides on cloud computing and the law for IT; for senior management and policy makers; for users
3. Cloud computing contracts, service level agreements and terms and conditions of use.

In the US, the Legal Cloud Computing Association[14] was formed in December 2010 as a consortium of leading cloud computing providers with a charter to:

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

- provide a unified and consistent voice for vendors in the legal cloud computing market;
- collaborate and cooperate with Bar Associations and other policy-forming bodies in efforts to form policies and guidelines relating to the use of cloud computing in law practices;
- define standards and best practices; and
- provide educational resources to attorneys and the broader legal community on cloud computing and the technical, legal and ethical issues relating to cloud computing.

While all the above scenarios indicate steps in the right direction, they also help prove that though the cloud has been around for some time, there is still a lot that needs to be researched and understood before taking to the cloud.

4.2. War in the Cloud

Clouds move due to various reasons, such as for business continuity during natural or man-made (such as wars) disasters, and cloud providers have to be very clear on where the data will move to and how the local jurisdiction will affect the customer. Some questions that come to mind could be:

- Will cloud vendors comply with all the rules and norms of the land? What is binding them to do so?
- What will happen when disaster strikes and the cloud moves?
- Who has the control and what regulations will apply?

Keeping in view the complex topic of security, there are questions yet to be answered and there are things to be researched. Above all, it cannot be stressed enough to be legally aware of the facts and always have your legal experts at hand. It might not be wrong to say that cyber war will become easier because data is not with us and we do not have much control over it. Anarchy and confusion will grow in exponential proportions due to social media networks. It will be even easier to mobilize "free radicals"[15] to aid in the technological massacre of the new century. Control becomes the foremost issue during war times and the ability to retract data back to its source is an equally important question which must be well clarified in the contracts. Look at the few examples in the

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

above paragraphs and you will realize that there is more to cloud computing than we can fathom today. A couple of years down the line is a very short time for technological developments as well as criminal developments.

The world is a very different place today compared to what it was before the tectonic shifts in the geography of the lands. With the way our weather and atmosphere is changing, the only thing we can be sure about are many more natural disasters coming our way. Cloud computing will be greatly affected by these super-human factors which are beyond our control. If it can be of any solace, having a well-defined business continuity and disaster recovery plans are vital to any business more than ever now. The terms of these documents must be scrutinized for locale specific accessibility and information. Today is nothing different from those days when modern day banking began and people started using bank safety vaults to store their secrets, savings and investments. If it is too personal and puts someone in jeopardy– don't store it in the cloud. Better yet, consider why do you even have such sensitive information in the first place and see if you can avoid using that data and instead use something less sensitive. This is where the guidelines and standards come into play. Have information auditors evaluate your business impact level and your data classification levels. Ensure that the analysts who deal with such data are well documented and security cleared and a non-disclosure agreement wouldn't hurt either. Above all, have faith but don't stop doubting.

5. Proposals, Recommendations and Solutions

5.1. Behavioral

Be cautious. Better yet! Be paranoid. Make sure to check and reaffirm before committing. Better to be safe than to be sorry paradigm applies more than ever now. Although trust is a very important factor in businesses, it also is important to keep our doubts and act upon them by taking preventive measures. Even if you are a risk taker, that is no reason to overlook the legal landscape of the regions that your clouds will exist in. Although move to the clouds might seem like a very ludicrous deal today, long term planning in terms of reliability, control and security should be at the forefront of any enterprise aiming to move their resources to the cloud providers. No more can the

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

managements afford to ignore the facts and be blindsided due to complacency or get away with the blame game. With all due respect to the famous poet, Thomas Gray, in the field of cloud computing though, **Ignorance is not bliss!**[16]

5.2. Legal and Lingo

The author of this paper is not a lawyer. You may not be a lawyer and even if you are, do not fail to employ a team of lawyers who will work and provide you with the much needed good night's sleep – it is worth all the trouble and money in the end. Have everything in black and white and in a safe place. It cannot be stressed enough that having a physical backup of critical data is very important even in cloud computing simply because of the fact that clouds move.

N.B. Terminology can mean a lot, so make sure you know your English well and have your glossary of terms updated each time you change the contract! If **N.B.** took some of you readers by surprise don't worry, you are not alone.

India, USA and the UK all have different legal tone - even the English! For example N.B. may not be such a common abbreviation in the U.S. whereas it is quite common to use the short form in British English or Indian English. So English differs too. Be careful what you write and what you want to mean. British English, Indian English (or its famous Indianisms) and American slangs all can either mean a lot or nothing when it comes to litigations. Choose your words as you would choose your financial investments.

Now, for the laundry list. Given below is a simple 44-point cloud check list of things-to-do when considering to cloud-source your data. Watch for the "fine print", local lingo and technical jargon, keep it simple and have everything in black and white because when it comes to litigation nothing speaks better than your contract.

Consider these simple tips before you commit your data.

1. How reliable are the network infrastructure?
2. How reliable are the physical locations against a political backdrop?
3. How strong is the local jurisdiction? Who has control over the cloud-based infrastructure?

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

4. How easy it is for bureaucracy to make its way into accessing the resources?
5. Ask for the transparency policies of the enterprise or the cloud provider.
6. What are the terms in the contract and what is the credibility of the person(s) making the commitments in the contract?
7. How long has the company been in the IT market? Ask for strong references from clients with similar efforts.
8. Check the company's Information Security Policy and make sure it fits your bill or discuss any changes upfront and be sure to mention the differences in the contract.
9. Do not mind asking about network breaches, Information Risk Assurance policies, Standards and guidelines.
10. Also, it is a good idea to have the company do a proper credit check for its employees who will be dealing with sensitive or critical data.
11. It is also a good idea to check the local area to get a feel of security outside the company.
12. Company retention policy, employee satisfaction rates, employee movement also matters when considering services because a happy employee is an asset, a disgruntled one can be a safety risk.
13. Consider nepotism. Nepotism can lead to corruption and corruption is to an enterprise what cancer is to human body!
14. A proper background check must be performed by a 3rd party to ensure the authenticity of the service provider and its people.
15. Every term must be clearly and explicitly spelled out in the contract in black and white to avoid any future issues.
16. Penalties in the event of non-compliance must also be very clearly included with specific mention about what is not included.
17. Operations and records must be audited, validated and reinforced periodically.

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

18. It is also a good idea to check for local law system prevailing in the area that the server is hosted
19. Perform cloud computing risk assessments as a pre-requisite and ongoing process
20. Check vendor's affiliations with major standards organizations, certifications and expertise level
21. Make sure the SLA's and all the contract terms are applicable to you and not just a copy-paste version from another client's contract. Avoid use of common and collective nouns, adjectives or adverbs in the contract. Use as simple, straightforward terms as possible.
22. Check and ensure proper disaster recovery procedures exist and the company's business continuity planning is up to date and effective.
23. Ask about all the regions the data would travel in case of a disaster or an incident.
24. Ask about the data handling procedures and the fine prints of the respective jurisdiction.
25. Check the access control list for the cloud services provider so you know who all will be handling your data and to what extent.
26. Have a contract in place to ensure safety of your data against any possible data mining or reverse engineering by the provider or by the data handlers.
27. Make sure you have and you understand the designations and their role in handling your data and ensure a direct line of communication at all times, so you know who can be contacted when you need something.
28. Check and ensure the providers are up to date on patching and enquire about their automatic patching methodology and how it can be customized for your company. Also ask about their emergency patching services.
29. Ask about their green initiatives, energy factors and carbon footprint.
30. Make sure their messaging and collaboration services are what you would expect. State your communication needs clearly and negotiate upon a clear path of information exchange.
31. Look into their Records Management strategies and make sure you both (Customer and the Cloud provider) mutually agree terms, based on the legislative requirements to retain records.

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

32. Check and enquire about their data destruction policies. Any inconsistencies or differences between jurisdictions must be well documented.
33. Make sure you are satisfied with their security policy and their encryption/decryption policies as well. All though it is highly depending on the local jurisdiction, it is very important to ensure consistent information.
34. Enquire about their Forensics expertise and incident handling experience.
35. It is very important to have a clear responsibility matrix in form of a Responsibility Assignment Matrix or Linear Responsibility charts etc., and ensure that both sides i.e., you and your cloud service provider have an up to date version of the same.
36. Discuss and clearly formulate a well documented event/incident/network logging mechanism in accordance to external standards legislative needs.
37. Run or thoroughly inspect their network architecture and infrastructure for mitigation techniques, isolation levels, critical network paths and their security configuration. Ensure any changes are clearly and promptly communicated to you as defined in your communication plan.
38. It would be a good idea to check out their Security Surveillance and Monitoring plan with the cloud providers and also look into their Perimeter Security Systems and the data access rules by any 3rd party.
39. Times change and relationships turn sour for various reasons. Make sure you have clearly written terms of dis-engagement, termination and data hand over procedures.
40. Secure coding practices are very important now more than ever.
41. Security awareness is equally important in all respects. Whether it is educating your children with a simple concept of "Stranger Danger" and checking your Facebook privacy settings every month or setting up the ADT system around your house and having a cop for a friend – every little thing works. It's better to be safe than to be sorry!
42. Restrict giving out too much information, from Facebook to phones and happy hours to Saturday night parties – every place is filled with eavesdroppers who are willing to go that extra mile to know about you. So, think before you talk and

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

keep in mind the 5W and 1H principle (Who, What, Where, When, Why and How). Seems like a lot of thinking before you can say "Hello" but it only takes seconds to a trained brain.

43. If it is important think twice before you take it – do you really need that information or can you substitute it with something that is not so critical?
44. Finally, use technology to its fullest potential. Use safety features in phones, on websites, around properties and your community. Use stronger passwords, pin numbers, and clever code words to identify yourself to your friends and family (Helps with children too!). Use multiple levels of security to safeguard yourself, your surroundings and likewise your data/assets.

5.3. Global Cloud Data Services©

One option is to create a common cloud legislation that will be even across regions. It should be based on objective measures and not tied up to any particular country or political regime. Consider this for a thought: The clouds could possibly be governed by the **G**lobal **C**loud **D**ata **S**ervices© body which could be made up of subject matter experts from the industry across the globe from areas such as linguistic, legal, IT, Network, Security, Market and Trade, Financial and Academia with powers something similar to the World Trade Organization, World Health Organization, Interpol or the United Nations to provide more uniform, neutral and global legislation, overall guidance and support. There are institutions from every country such as Data Security Council of India, European Union in the EU, the Federal Trade Commission and the Department of Homeland Security in the USA, the Wassenaar Arrangement, the World Intellectual Property Organization (WIPO) and not-for-profit organizations such as the Cloud Security Alliance (CSA). The challenge will be to get these global bodies together and also the local authorities from each of these countries such as National Institute of Standards and Technology, Information Commissioner's Office (ICO) to form a set of common guidelines and laws for the clouds which can be objectively administered across nations. This body will be responsible for uniform cloud data governance. They can take their inputs from their local counterparts - but only recommendations – the body will have the authority to make or mend the law. They will also be responsible to govern

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

uniformity across cloud providers through guidance and support. The GCDS formation itself will be a rigorous process taking experts through a well defined selected process transparent to the nations and will operate for a certain pre-determined contractual period after which new members will be chosen to bring in fresh ideas! As such laws of every land as different due to the basic fact that each of these lands are geographically, culturally, politically quite different from each other. While it is important to maintain this identity, it is also important to unify some of the laws to provide a neutral ground to base our future disputes on. Given the fact that technological warfare will continue to evolve, so should the legalese.

5.4. Educational and Academics

Many universities and schools all over the world are slowly but steadily moving their IT infrastructure to the cloud. Software giants like IBM©, Microsoft©, Google© and EMC© have a sleuth of products aimed at students and teachers and the way education is imparted in schools and universities. The selling point has always been the cost of infrastructure and maintenance that the universities can save. Though the selling point is not new to the concept of the cloud, the buy in from universities is obvious as this cost saving directly impacts the funds available to the universities for other activities.

While the cost advantages are obvious there is also a definitive need to look at other aspects of moving to the cloud. Among these other factors, security is of prime importance. Security and data protection has always been at the core of the educational system in many countries and various laws like Family Educational Rights and Privacy Acts (FERPA) in the USA and European Directive on Protection of Personal Data (Directive 95/46/EC) in Europe determine the laws of data sharing and student parent rights that schools have to abide by.

So what do universities consider when they make a plan to move to the cloud? According to the chief information officer of the University of Montana, Dr. Lenn Knapp "From a legal perspective, privacy is very important to us. We need to be FERPA and Americans with disability Act (ADA) compliant and Microsoft's contract language is very clear. With Live@edu, we are confident our students' data is fully protected. We know and can control who has access to the data, and we have assurances that the data

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

won't be mined." (Microsoft, 2010). Cloud providers also realize the need to fulfill these requirements and have been working on their own proprietary methods to achieve compliance.

For example:

The EMC education cloud includes significant levels of data security by combining OSSEC with technology from EMC's RSA ® security division. OSSEC is a free, open source, host based intrusion detection system (IDS) that will detect malicious attacks against the site. In addition to Google Apps' built-in email security, Google offers an additional range of protection through its Postini security and archiving services.

Microsoft's Exchange Hosted Services offers online tools to help your organization protect itself from spam and malware, satisfy retention requirements for e-discovery and compliance, encrypt data to preserve confidentiality, and maintain access to email during and after emergency situations.

Apart from providing cloud based solutions, the big corporations have also been investing in schools and universities to fund research and development in the area of cloud computing. Programs like Cluster Exploratory program (CLuE) and Trustworthy Virtual cloud computing granted by National Science Foundation (in the USA), the EGEE (Enabling Grids for E-sciencE) in Europe and the ACCI (Academic Cloud Computing Initiative) by IBM/ Google are some examples of these initiatives.

In April 2009, the National Science Foundation announced it had awarded $5 million in grants to fourteen universities as part of its Cluster Exploratory (CLuE) program. The program works with IBM and Google on their Cloud Computing University initiative, and is designed to look at the infrastructure requirements to make leading-edge cloud computing system which many believe will power the next generation of the World Wide Web. IBM Google and Microsoft have released millions of dollars in grants to universities for cloud computing research.

The introduction of cloud computing saw the major universities evaluate and start using cloud based solutions as a means of reducing cost. Cloud based email servers were an instant hit and solutions like Live@edu have been accepted by universities and schools

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

all over the world. Slowly but steadily cloud based applications in the area of education have emerged and are being tried out in different countries all over the world.

Microsoft©, IBM©, Google© and EMC© among others have also been fighting hard to capture the lucrative and endless market of the education sector. Along with investing in research and development in this area, these giants have also been investing in these universities and schools to produce the work force required to develop the next generation of cloud based applications.

As early as October 2007 Google and IBM announced an initiative to promote new software development methods to help address the challenges of internet-scale applications. The goal of this initiative was to improve computer science students' knowledge of highly parallel computing practices to better address the emerging paradigm of large-scale distributed computing.

Universities all over the world have started providing specialized courses in cloud computing. On September 15th 2011, the Minister of Education and Skills, Ruairi Quinn, TD met with some of the students of the world's first industry-led cloud Masters Degree Program being offered by the Cork Institute of Technology in association with EMC. This unique program has been initiated with 64 students out of which 25 of them are EMC employees. In the UK, University of Aberdeen and Sheffield Hallam University are the first to offer M.Sc degrees in the area of cloud computing. The courses span over 12 months and are aimed at preparing students for the demands of the cloud computing industry which has been touted as the next big thing after the invent of the internet. The course specification on the University of Aberdeen's website also states that the requirements include strong programming skills using JAVA. The course content on the Sheffield Hallam University website also includes importance to other areas of the cloud. It states:

"You also investigate the commercial, legal and social implications for businesses, the use of distributed computing environments, and how they provide seamless interfaces to scalable high-performance computing resources" (Sheffield Hallam). This shows that there is an emphasis on other aspects of the cloud but the question remains if it is enough.

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Another hot topic of debate has been that of modern day "agile" programmers and their approach towards software engineering. Many of us might remember the days of nuts and bolts – of tightly structured languages which left everything in the hands of the programmer from declaration of memory to garbage collection. Although the importance of speed and agility in this day and age is crucial, it is equally important to be well informed. In the yester years, you had to have "the stuff" to do real programming and the title "programmer" evoked a whole different feeling in us and filled us with some sense of responsibility and pride. With all due respect to JAVA, the modern day JAVA programmer has taken many areas of application development for granted based on what JAVA promises to handle. These programmers are quite different in their approach towards software engineering and although object oriented programming started off on a different note in languages such as Smalltalk, C++ or Object Pascal, it took a whole new turn with the advent of JAVA. The core approach of having to dot every "i" and cross every "t" has been taken over by automatic garbage collectors and run times. Although the concept of encapsulation was the "wow factor" in the 90's, it became a way of life later on and software developers since then have almost ignored bothering themselves with the details of how parts of the program worked. A powerful language like JAVA can accomplish a lot in the hands of great software developers. Understanding how everything works together is a very important part of building anything worthwhile.

An initial scan of the course contents offered by different educational bodies does not reveal imparting knowledge of these rules, regulations and core aspects like security and a good programming paradigm. Now more than ever, it is of prime importance to learn good programming practices and build security "into" the software rather than just worrying about "security on top" – security is not a butter cream icing on the top! Secure programming will aid in cutting down the incidents and security breaches. Last but not the least, sloppy programming and sloppy programmers must be just as penalized as the cyber crime offenders. It's as dumb as locking up a plastic safe with heavy metal locks!

From a business perspective will businesses readily rely in these new generation programmers to develop business critical applications while maintaining the rules of the industry and the regulations set by the government across borders? Time does not have

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

answers to these questions. We do. The industry professionals have to work together with academic institutions and help them train the programmers of the future.

6. Conclusion

While this paper gives a fairly brief overview on some of the laws across the three borders, India, USA and UK, there are also other countries on the World Wide Web today and many more that will join in, thus increasing the trials and tribulations of the law keepers. Apart from the worry that IP addresses may not be sufficient for the future and the hope that IPv6 will provide enough addresses for all the people on this planet for all the devices, we also have to worry about getting along with each other in this one big happy family called the "internet", with reluctance though. It sounds like a roller coaster experience of some crazy adventure park as, while we were busy getting ourselves compliant with PCI–DSS' requirements with consumer payment data, we were also worried about the whistle blowers[17] and the phone hacking scandals (BBC News, 2011). At the same time, we cannot forget how earlier this year we heard of Egypt shutting down its internet access to scores of its people (Bradshaw, 2011) and after that we also read about how media contributed both positively and negatively to the infamous London riots of 2011 (BBC UK, 2011). During all this, we constantly tried to be more efficient and cost-effective and invented various technologies such as virtualization and cloud computing, which seemed to erase all technological boundaries of the internet invariably bringing in floods of legal and security issues from all over the world into a common pool. Nevertheless technologies evolved and so its tenacious grip on us humans tightened through wireless devices, smarter computer chips and cheaper storage devices. We were all connected more than ever now and could store huge amounts of data that could have been quite expensive to possess a few years ago. Whether we needed the data or if we had the right to own it, did not matter. It was out there and we felt a natural instinct to own it. This was a major boost to those who wanted to exploit this "technological freedom".

With each passing day, there are many instances of how these inventions and technological advancements are crippling our ability to function as moral beings and are instead aiding in causing troubles to ourselves. Education and security awareness play an

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

extremely important role in today's world, lack of which will only cause anarchy and utter disrespect to the laws of the land. The instances above are mere glimpses of the "power of the internet" and they are more than enough to jolt us out of the dreamy clouds. But fear and avoidance are not an option anymore. We have to face the "internet daemon" (and it is no spelling mistake!) head-on which means that we have to work with data on a whole new level. This paper can only conclude to **Take only what's needed and protect what you have, from inside and out.** Data is more valuable today than information, because it is this data that can be collated in various forms to give information about anything and everything that lies on the World Wide Web.

We have sustained the IT we inherited from the baby boomers, it's time to do our share and give the 21st century a stronger and safer IT to live in and make the father of the WWW, Sir Tim-Berners Lee proud! (W3).

Make Security your way of life

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

7. References

Mell, P., & Grance, T. (2011). US Department of Commerce, National Institute of Standards and Technology. The NIST definition of cloud computing Retrieved from http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

Hogan, M., Liu, F., Sokol, A., & Tong, J. (2011). US Department of Commerce, National Institute of Standards and Technology. NIST cloud computing standards roadmap – version 1.0 Retrieved from http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909024

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). US Department of Commerce, National Institute of Standards and Technology. NIST cloud computing reference architecture Retrieved from http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

SourcingLine. (2011). Global sourcing & outsourcing locations. Retrieved from http://www.sourcingline.com/outsourcing-location/india

National Informatics Center. (2011). The constitution (seventy-third amendment) act, 1992. Retrieved from http://indiacode.nic.in/coiweb/amend/amend73.htm

India Against Corruption. (2011). About Lokpal. Retrieved from http://www.indiaagainstcorruption.org/salient.html

India Against Corruption. (2011). Jan Lokpal bill a detailed analysis. (1.0 ed., p. 29). Retrieved from http://www.indiaagainstcorruption.org/docs/Jan_Lokpal_Bill-A-Detailed_Analysis.doc

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Overby, S. (2011, July 14). How to resolve disputes with your outsourcing provider. Retrieved from http://www.computerworlduk.com/how-to/outsourcing/3291296/how-to-resolve-disputes-with-your-outsourcing-provider/?intcmp=rel_articles;outsrcng;link_6

Ministry of External Affairs, Government of India, ITP Division. (n.d.). Intellectual property rights Retrieved from http://www.indiainbusiness.nic.in/investment/ipr.htm

Chapman, S. (2009, January 13). Satyam fraud scandal: timeline. Retrieved from http://www.computerworlduk.com/how-to/outsourcing/1982/satyam-fraud-scandal-timeline/

Whittaker, Z. (2010, July 29). Blackberry encryption 'too secure': national security vs. consumer privacy. Retrieved from http://www.zdnet.com/blog/igeneration/blackberry-encryption-too-secure-national-security-vs-consumer-privacy/5732

Singh, V. K. (2010, August 3). Encryption standards, norms and laws in india [Web log message]. Retrieved from http://cyberlawsinindia.blogspot.com/2010/08/encryption-standards-norms-and-laws-in.html

Nair, N. K., Barman, A. K., & Chattopadhyay, U. Government of India, Ministry of Human Resource Development. (1999). Study on copyright piracy in india Retrieved from http://copyright.gov.in/Documents/STUDY ON COPYRIGHT PIRACY IN INDIA.pdf

National Informatics Centre, N. Ministry of Communications & Information Technology, Department of Information Technology. (2010). Literacy Retrieved from http://india.gov.in/knowindia/literacy.php

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

Runckel, C.W. (2007). India and china - looking below the surface to compare these two rising asian business giants. Retrieved from http://www.business-in-asia.com/asia/comparing_china_india.html

Tiwari, A. (2011, June 12). Electricity crisis in india [Web log message]. Retrieved from http://www.electricityinindia.com/

CRID. European Commission, University of Namur. (2005). First analysis of the personal data protection law in india Retrieved from http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_india_en.pdf

Sandfiorenzo, L. (2011, July 13). 2011 Indian privacy law. Retrieved from http://www.outsourcing-law.com/2011/07/2011-indian-privacy-law/

Kerr, O. S. (2004). A user's guide to the stored communications act, and a legislator's guide to amending it. Informally published manuscript, Law School, George Washington University, Washington, D.C., USA. Retrieved from http://ssrn.com/abstract=421860

Information Commisioner's Office, (n.d.). Freedom of information faqs -for organisations Retrieved from http://www.ico.gov.uk/Global/faqs/freedom_of_information_for_organisations.aspx

Sullivan, B. (2006, October 19). 'la difference' is stark in eu, u.s. privacy laws. Retrieved from http://www.msnbc.msn.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/

HMG, Cabinet Office. (2008). Hmg security policy framework Retrieved from http://webarchive.nationalarchives.gov.uk/ /http://www.cabinetoffice.gov.uk/media/111428/spf.pdf

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

DOE. Department for Education, News and Press Notices. (2011). New guidance for teachers to help improve discipline in schools Retrieved from http://www.education.gov.uk/inthenews/inthenews/a00191991/new-guidance-for-teachers-to-help-improve-discipline-in-schools

News Press Release. (2010, January 20). Microsoft urges government and industry to work together to build confidence in the cloud. Retrieved from http://www.microsoft.com/presspass/press/2010/jan10/1-20brookingspr.mspx

Webmaster. (n.d.). QMUL cloud legal project. Retrieved from http://www.cloudlegal.ccls.qmul.ac.uk/

JISC. (2011, August 31). Jisc legal cloud computing and the law toolkit (31/08/2011). Retrieved from http://www.jisclegal.ac.uk/ManageContent/ManageContent/tabid/243/ID/2135/JISC-Legal-Cloud-Computing-and-the-Law-Toolkit-31082011.aspx

Microsoft. (2010, October 04). Universities go back to school with live@edu. Retrieved from http://www.microsoft.com/presspass/press/2010/oct10/10-04msliveedumomentumpr.mspx

Sheffield Hallam. (n.d.). Msc web and cloud computing. Retrieved from http://www.shu.ac.uk/prospectus/course/1064/content/

BBC News, (2011). Phone-hacking scandal: timeline. Retrieved from http://www.bbc.co.uk/news/uk-14124020

Bradshaw, T. (2011, January 28). Condemnation over Egypt's internet shutdown. Retrieved from http://www.ft.com/cms/s/0/08dbe398-2abb-11e0-a2f3-00144feab49a.html

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

BBC U.K. (2011, August 25). Social media talks about rioting 'constructive'. Retrieved from http://www.bbc.co.uk/news/uk-14657456

W3. (n.d.). Tim Berners-lee. Retrieved from http://www.w3.org/People/Berners-Lee/

Econsultancy. (2011, October). Global internet statistics compendium. Retrieved from http://econsultancy.com/uk/reports/global-internet-statistics-compendium

Internet World Stats. (2011, October). Internet users in the world. Retrieved from http://www.internetworldstats.com/stats.htm

Esipova, N., Ray, J., & Srinivasan, R. (2010, April 30). Young, less educated yearn to migrate to the u.s.. Retrieved from http://www.gallup.com/poll/127604/young-less-educated-yearn-migrate.aspx

Bhuta, J. (2010, November 23). Clicked: my views on photography. Retrieved from http://jesalb.blogspot.com/2010/11/article-i-found-on-silly-photography.html

Internet usage stats and telecommunications market report. (2011). Retrieved from http://www.internetworldstats.com/asia/in.htm

companies House. (n.d.). Information and guidance. Retrieved from http://www.companieshouse.gov.uk/infoAndGuide/companyRegistration.shtml

MS News Archive. (2011). Microsoft news center. Retrieved from http://www.microsoft.com/presspass/exec/bradsmith/?tab=speeches

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Footnotes

[1] http://www.copyright.gov/title17/circ92.pdf

[2] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf

[3] http://www.state.gov/documents/organization/128321.pdf

[4] http://rti.gov.in/webactrti.htm

[5] http://www.ichay-mullenex.com/download/india-implements-brand-new-data-protection-laws.pdf

[6] http://www.rsa.com/rsalabs/node.asp?id=2330

[7] http://www.wassenaar.org/controllists/2010/WA-LIST%20%2810%29%201%20Corr/WA-LIST%20%2810%29%201%20Corr.pdf

[8] http://www.mosi.org.uk/media/33871840/electricityinbritain.pdf

[9] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

[10] http://www.cesg.gov.uk/products_services/iacs/clas/index.shtml

[11] http://www.sirimo.co.uk/2009/05/14/uk-photographers-rights-v2/

[12] http://www.krages.com/phoright.htm

[13] http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[14] http://www.legalcloudcomputingassociation.org/

[15] Free Radicals is a term coined by author to refer to the anti-social elements in our society who are ever ready to latch upon the slightest chance to team up against the government just for the fun of it sometimes.

[16] http://www.thomasgray.org/cgi-bin/display.cgi?text=odec

[17] http://en.wikipedia.org/wiki/Julian_Assange

Godha Iyengar, Godha.iyengar@yahoo.com

© 2011 SANS Institute, Author retains full rights.

Last Updated: May 26th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**