



Tony Richardson

Tony.richardson@octree.co.uk

Monday, 07 March 2011

Does cloud computing improve security for the SME ?



Index

Executive Summary	4
Introduction	5
Cloud Computing Defined	6
IT Governance	7
Access Control	8
Physical and Environmental Security	9
Cryptography	11
Legislation, Regulation and Compliance	12
Application Security	13
Business Continuity and Disaster Recovery	14
Conclusion	15
Bibliography	16
Appendix	18

About the Author

Tony Richardson has been involved in information technology for 29 years. Originally trained as a Management Accountant he has developed a broadline knowledge of technology within numerous industry sectors. He founded an IT solutions provider – Octree Computers - in 1990, and continues to provide expert technology solutions to the Small Medium Business community (organisations up to 250 employees who have little or no in-house expertise) with a specific focus on Information Assurance in the professional services sectors – financial, accounting, legal, creative, and architectural.

Tony has achieved CISSP (Certified Information Systems Security Professional) certification, the first credential in the field of information security accredited by the ANSI (American National Standards Institute) to ISO (International Standards Organization) Standard 17024:2003. CISSP certification is not only an objective measure of excellence, but a globally recognised standard of achievement, and is presently held by less than 70,000 professionals worldwide.

Tony holds a Certificate in Microsoft Technologies gained at Lancaster University, and is a member of the Microsoft Partner Research Panel, a Microsoft Certified Professional, and a consultant for the Reuters Insight Community of Experts. He is an associate of IT Governance specializing in ISO27001 ISMS implementation. He actively pursues a program of continuing professional development through vendor specific, and vendor neutral training and accreditation.

Tony is presently studying for his Masters' Degree in Cyber Security at Lancaster University.

Tony can be contacted by email at tony.richardson@octree.co.uk

Cloud Computing Increases Security?

Executive Summary

Cloud computing certainly appears to be the buzzword of the day, and will continue to be so. It represents a quantum shift in the way IT services are procured and delivered. And there is no doubting the significant operational advantages that it offers such as instant scalability and performance, as well as the potential for considerable savings in infrastructure costs, licensing, IT support personnel and simplification of the computing complexities of internal systems. It is estimated that only 6% of the total computing power of an organisation is consumed at any one time (The Economist, 2008) with the slack being utilised for infrequent spikes in demand, so what if that spare capacity could be put to greater advantage? Or the costs associated with powering and operating this unwieldy infrastructure negated? Today 70-80% of IT expenditure relates to the operation and maintenance of existing infrastructure and legacy applications.

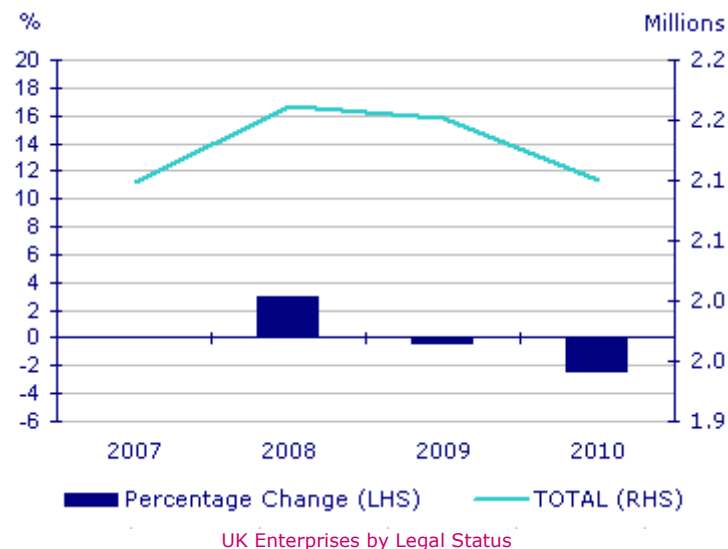
However these clear pecuniary advantages may well, no pun intended, be clouding the judgment of the CEO and CFO, particularly those early adopters who have not performed due care and due diligence when migrating to a cloud environment. We may well learn significant lessons from such zealots. And to suggest cloud computing increases or decreases security depends on the context of the existing security within the organisation, the critical sensitivity of information and applications, the nature of the business, and indeed it's legal and regulatory obligations. What it does provide are new risks and new opportunities.

Introduction

Let's look at the security and information technology needs and resources of the Small Medium Enterprise (SME - those organisations with fewer than 250 employees) in the UK. This group represents a significant proportion of UK businesses - more than 2 million according to the Office for National Statistics- (Office for National Statistics, 2010):

Businesses

Number of UK Businesses down



These organisations invariably lack in-house resources or expertise for delivering and maintaining effective IT environments. This alone suggests “cloud Computing” is an attractive alternative to deploying in-house infrastructure. We shall see.

In larger organisations the financial advantages are more obvious. According to research carried out by Dr.Howard Rubin (Hulitzky, 2011), a researcher in techno-business strategy and global software economics, and Professor Emeritus of Computer Science at Hunter College of the City University of New York, only 30 to 35 percent of all IT expenditure is variable cost. His IT Commons concept suggests companies can achieve 60 percent or more variability on IT operating expenses by reducing unused IT infrastructure capacity, thus resulting in more money available for developing current systems instead of reverse investment maintaining legacy systems. However security does not appear to be a consideration in his analysis.

And whilst there remains no information security standard framework for cloud computing, for the purpose of structure I will reference key elements of the Common Body of Knowledge of ISC2, and the Cloud Security Alliance’s “Security Guidance for Critical Areas of Focus in Cloud Computing” (www.cloudsecurityalliance.org) where relevant.

Cloud Computing Defined

It is now widely accepted that cloud computing can be defined within the following three service levels, commonly known as the SPI model (Cloud Security Alliance, 2009):

Software as a Service (SaaS) – where the service provider hosts an application without the user having to internally host and support the application.

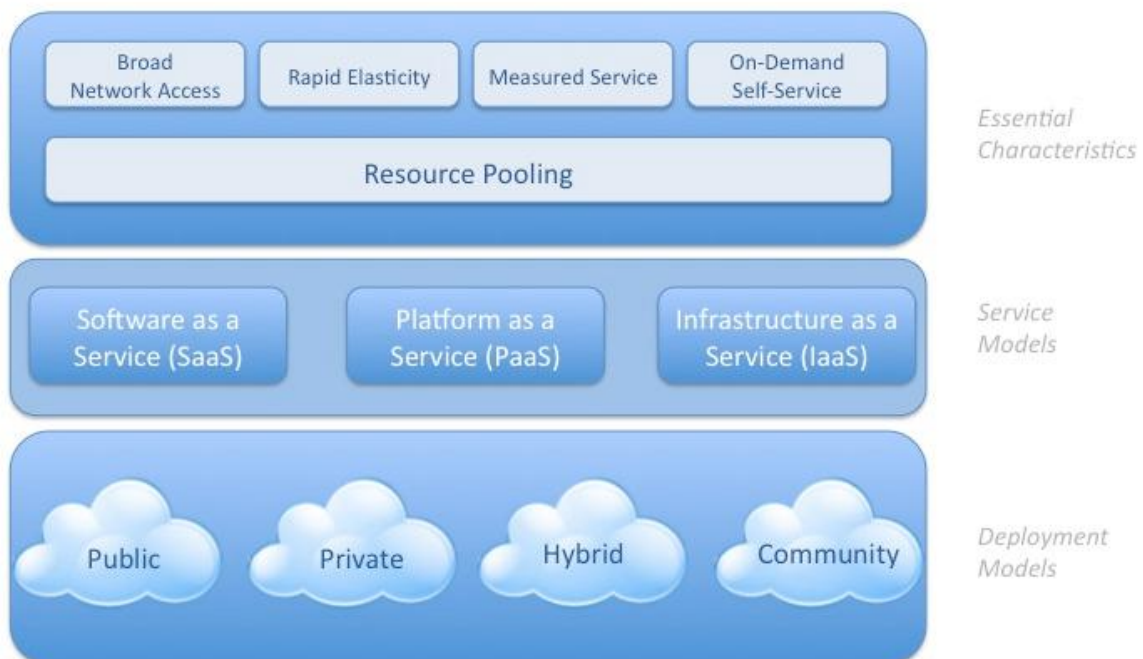
Platform as a Service (PaaS) – where the service provider hosts a development environment so the customer can create and develop applications on a provider's computing environment eliminating the need for in-house infrastructure.

Infrastructure as a Service (IaaS) – this allows a customer to rent a computing environment, such as a datacentre or storage environment, without the need to create and maintain the resource internally.

The U.S. National Institute of Standards and Technology (NIST) further defines cloud computing to incorporate five characteristics and four deployment models as shown below. The delivery of utilities such as electric power is analogous to the cloud computing concept in as much as the user consumes as much or as little of a particular resource as required at any given time, exploiting the elasticity and scalability of the provided environment, further enhanced by the maturity of virtualisation technology.

Visual Model Of NIST Working Definition Of Cloud Computing

<http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html>



IT Governance

At the very foundation of all information security management systems is the over-arching security policy as endorsed by senior management, and communicated to all employees, highlighting the responsibility of all staff members, whatever their role, to uphold the security obligations and directives of the organisation for the good of the organisation, its staff members, its clients and any third party or stakeholder. It outlines, without going into any great detail, what is to be protected (the company's information assets) and why, countermeasures that may be in place, and the consequences of non-adherence, both to the organisation and any individual. As a document that requires only periodic review it presents more of a mission statement, with individual detailed policies relating to specific elements, such as password management and USB device control, being derived from it. It is certainly true that very few SMEs develop effective information security policies – 66 percent of all security breaches in the last 18 months came from businesses employing less than 100 people (Murray, 2010) - and even fewer deploy measures for policing those that are introduced as a token gesture. Some do attempt to apply Acceptable Usage Policies (AUPs) to try to minimise the abuse of computer systems for nefarious or non-work related activities, often implementing cloud based security services.

In order to develop appropriate policies and procedures it is essential to carry out extensive risk analysis, identifying all information assets, classifying them, and determining the potential threats to and vulnerabilities within them. Are those threats and vulnerabilities likely to change when moved to the cloud? Almost certainly. It is therefore essential to choose your cloud service provider wisely and analyse their security policies to ensure they also meet your requirements, both operationally and for regulatory compliance purposes. We have seen recently the impact of the Distributed Denial of Service (DDoS) attacks by the group Anonymous on Amazon, Mastercard, the Bank of America, and some online anti-piracy and entertainment sites as a result of the Wikileaks scandal (Infosecurity Magazine, 2011). What if you happen to place critical information assets with a service provider also hosting a targeted entity because of their actions or beliefs? Can the service provider negate such an attack that may indiscriminately affect your operations?

It is, of course, very likely that a mature cloud service provider will have a far more comprehensive security architecture, policies, processes and staff in place way beyond the capabilities of the average small business. Google employs more than 175 security staff, and how many organisations are able to afford such a resource?

Access Control

Access control relates to the identification, typically a username, and authentication, usually a password, of users or processes for the purpose of accessing or executing a network program or resource, such as application data, printing to a network printer, opening a file or folder, for example. Microsoft Windows environments utilise Mandatory Access Control (MAC) meaning that the operating system kernel determines access rights dependent on pre-determined access control lists as configured by system administrators. Users and data owners do not determine access privileges to information or resources as would occur in Discretionary Access Control (DAC) environments.

Whilst identification is usually public domain information it has to be unique for accountability purposes. And accountability is a key factor within information security management. Authentication is usually performed using one or more characteristics or pieces of information known solely by the user being authenticated, i.e.

- Something You Know (a password)
- Something You Have (a token such as a smartcard, or certificate)
- Something You Are (biometrics such as retina scan or fingerprint)

The human factor in information security is very often overlooked, at least within small businesses where an assumption that technology will solve all security issues prevails. It is also true that computers do not commit crime – people do (Lacey, 2009). Technology is installed, configured, managed and operated by people who can and will make mistakes – whether it is as a result of carelessness, apathy, intent, accident, malice or a more nefarious activity. Social engineering techniques are employed by extremely convincing threat agents, such as spam phishing emails, calls for password information to helpdesks, “tailgating” at the business boundaries. The people we need to authenticate and control, in the context of security, are no longer just internal employees of the business, but partners, associates, visitors and even customers. In the age of the “de-perimeterised” network (Schneier, 2010) this is an increasingly difficult challenge. By moving to a cloud environment this identity conundrum can be alleviated somewhat as the cloud service provider is likely to be better equipped, financially, technologically and resourcefully, to address these concerns and to be able to monitor them. Yet it is critical to ensure the provider of choice is suitably covered. However administrative staff within the service provider itself will also potentially have access to the “crown jewels” and need to be carefully managed.

Physical and Environmental Security

One thing for sure is that any service provider worth his salt who intends to establish longevity and business success will be investing heavily in state of the art facilities, potentially in more than one geographical location, that incorporate the latest physical security technology and skilled personnel. They cannot afford not to, as any physical security breach at a high profile datacentre hosting facility could be catastrophic for the service provider. Such investment is unlikely to be made in small businesses, and often SMEs are in managed or shared office facilities less concerned with security beyond the legal and regulatory health and safety initiatives.

These cloud computing facilities will offer the latest in electronic surveillance systems, CCTV, physical device control on all perimeter entrances and exits, security passes, proximity controls, deterring fencing and lighting, fire suppression, even blast proofing techniques to protect against the terrorist threat, guards to challenge all entrants who may not meet all the necessary access control requirements, for example (taken from Amazon's AWS Security Whitepaper):

Physical Security

Amazon has many years of experience in designing, constructing, and operating large-scale datacenters. This experience has been applied to the AWS platform and infrastructure. AWS datacenters are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides datacenter access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to datacenters by AWS employees is logged and audited routinely.

Environmental Safeguards

Amazon's data centers are state of the art, utilizing innovative architectural and engineering approaches.

Redundancy

AWS data centers are designed to anticipate and tolerate failure while maintaining service levels, and are built in clusters in various global regions. All of AWS' data centers are online and serving traffic; no data center is "cold." In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and

electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Climate and Temperature

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels “ (Amazon Web Services, 2010)

Other considerations that have to be made include the proximity of emergency services and enforcement agencies, provision of utilities, landscape, and ease of access. Significant financial investment indeed, but essential nonetheless.

Cryptography

Some may argue that encryption is the answer to many of our security concerns and vulnerabilities. So what if our data is accessed as long as the keys remain secure, and sufficiently complex themselves? Few SMEs have any concept of protecting critical information assets by strong encryption. For example those organisations which handle and process personally identifiable information have to comply with The Data Protection Act of 1998, specifically Principle 7 which refers to data security (Information Commissioners Office, 2009):

“Make sure you have the right physical and technical security backed up by robust policies and procedures”

Whilst the Act is not specific about the technology required it implies that whatever means are considered appropriate and available should be implemented. According to Toshiba Information Assurance 71% of organisations claim to comply with the Act yet only 8% encrypt portable hard disk drives. The Financial Services Authority goes further in its Best Practices Guidelines to state that all “computers” that hold personally identifiable and employee data “must” be encrypted (Financial Services Authority, 2008). A similar approach needs to be adopted when transferring critical data to the cloud. But who is then responsible for managing the keys? The lower down the SPI (SaaS, PaaS, IaaS) cloud computing stack the implementation is, the greater the emphasis on the consumer to implement and manage security measures. Data can be transferred to and from the cloud securely over SSL connections using certificates issued by a trusted third party, such as Verisign or Thawte. Data at rest can be encrypted using a symmetric encryption algorithm such as AES (Advanced Encryption Standard) with variable key lengths.

This is also an important consideration when assessing the lifecycle of any application and system. What happens to the data when the system hardware is decommissioned? Encryption can be critical to the safe disposal of redundant hardware and media.

Legislation, Regulation and Compliance

Because of the geographically dispersed locations for cloud applications and data this can be a potential minefield, and presents many issues. There is a plethora of regulation and compliance mandates to conform to yet there remains little, if any, standardisation across the global jurisdictions who may be hosting your data. Data privacy laws in the USA may well be less stringent than the EU. The first thing to determine is exactly where your data is to be hosted, and replicated, and unless those jurisdictions provide the same level of data protection that you have to achieve you will need to review your cloud provider adoption. Some organisations have already fallen foul of their regulatory bodies as a result, for example Zurich UK was fined a record £2.25m by the FSA for failing to have the necessary protection and procedures in place following the loss of 46,000 client records in South Africa, something that did not come to light for 12 months (Financial Services Authority, 2010).

It must also be noted that very few of these laws and regulations directly reference cloud computing so can be open to interpretation. The PCI-DSS (Payment Card Industry Data Security Standard) is a global standard introduced to regulate the payment card processing industry and states 12 high level directives that have to be met (Vines, 2010):

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of card holder data across open public networks
- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications
- Restrict access to cardholder data based on the business's need to know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security.

Sounds like common sense? Unfortunately not everyone seems to agree. And the list of EU legislation is astounding. The table, in Appendix A (Bloor Research, 2009) details the many EU Compliance directives currently in operation.

Application Security

The cloud environment does present a fantastic opportunity for legacy applications, originally developed with little or no security considerations, being re-developed for this new platform to be written far more securely and conforming to the design principles that provide for “software assurance” (Vines, 2010, p. 66). It is common knowledge that security “bolt-ons” are costly and seldom effective. If the three principles of Dependability, Trustworthiness, and Resilience are applied from the ground up then there is a greater chance of significantly reducing the threat landscape in a cloud environment. If the SaaS provider can demonstrate such due care within their applications then this certainly is a step in the right direction towards more a secure computing platform. Additionally there are seven complementary principles to support information assurance, many of which have been touched upon in this paper:

- Confidentiality – prevent the unauthorised disclosure of information
- Integrity – ensuring that unauthorised modifications are not made to information
- Availability – ensuring that information and resources are available when required
- Authentication – guaranteeing identity
- Authorisation – applying the right privileges are granted
- Auditing – providing a snapshot and ongoing assessment of the system for control purposes
- Accountability – to be able to determine activities within the system to a specific user

Many small businesses will be utilising “off the shelf” application software with little or no customisation and therefore it may be relatively easy to migrate to a cloud environment where the likes of Salesforce.com, for example, are a major player and enjoy huge success in the CRM application arena. Office productivity applications are readily available from the likes of Google and Microsoft (Microsoft, 2011), and you have to assume that for these vendors security is absolutely essential for their continued success in this space.

Business Continuity and Disaster Recovery

For many the terms Business Continuity and Disaster Recovery mean the same thing. This is not true. Business continuity focuses on the resumption, or continued operation, of critical business functions, not necessarily at the original location, whilst disaster recovery concerns itself with the resumption of normal operations as they were prior to any crisis. Unfortunately this is another area often neglected by small businesses. Let's turn the clock back to the 1970's and the frequent power cuts as a result of industrial action, the hours of candlelight and lack of heat or hot food; how many of us could sustain a stable and reliable computing environment today if it was repeated? That may now sound extreme but who could have predicted the attacks on the World Trade Centre and their aftermath (Taleb, 2010)? It is the phenomenon of unpredictability, commonly known as Black Swan Events, which makes this facet of security an almost impossible task to compensate for the highly improbable.

“Had the risk been reasonably conceivable on September 10th, it would not have happened”.

Whilst the primary concern is always to protect human life the secondary goal is always to ensure the survival of the business. Cloud computing provides a fantastic opportunity for small businesses to move their information assets to a more resilient environment, assuming the cloud service provider can adequately demonstrate their business continuity management and disaster recovery plans confidently (see Appendix B for Amazon's Service Level Agreement (Amazon Web Services, 2010)), and allowing for widespread internet access from other locations and facilities can ensure normal business continues with little interruption or inconvenience.

For the purposes of business continuity critical business functions, and supporting systems, have to be identified, and a risk analysis performed. What are the threats to and vulnerabilities within your IT infrastructure, and information systems? How are you going to avoid, mitigate, or transfer these? Or do you just accept that they may occur and deal with it? This will provide a business impact analysis, at least for the purposes of planning and decision making.

The dramatic increase in mobile and home working also goes a long way to endorsing cloud computing consideration for business continuity purposes. Access at any time from anywhere to business critical applications and information is becoming a reality.

One obvious concern is the capability to migrate to an alternative service provider in the event that the relationship is terminated for whatever reason, or the service provider goes out of business.

Conclusion

The debate may well rage on, possibly indefinitely, however the march towards cloud technology adoption will continue unabated, irrespective of expert opinion, which I am pretty sure will also remain divided. The financial benefits are assumed to be too substantial to ignore. There are significant operational benefits too. And before writing this whitepaper I concurred that cloud computing did not increase security. I have changed my mind. I still have reservations, certainly for the SME in the UK, where there is a huge dependence on an aging communications infrastructure, and an even less healthy monopoly. Given that information security is founded on three fundamental principles – Confidentiality, Integrity and Availability – can anyone guarantee consistent availability of cloud based services? Our DSL broadband availability cannot be compared to the Service Level Agreements of cloud service providers such as Amazon, who “guarantee” 99.9% availability of their infrastructure (Amazon Web Services, 2010). And service level agreements are almost non-existent regarding Internet Service Provider DSL continuity. In Manchester in 2004 a fire in a BT cable tunnel paralysed the business community, costing an estimated £4.5m per day (Computer Weekly, 2004). In 2010 a fire at a BT node in Paddington caused major disruption to 437 local exchanges and up to 37,500 Datastream circuits (The Register, 2010). In fact 2010 saw a number of major service outages which left many small businesses without email and internet access for several days (Page, 2010). What would have been the implications and consequences of hosting their line of business applications and information assets in the cloud? Furthermore the Wikileaks scandal, that saw a number of high profile organisations targeted with Distributed Denial of Service attacks orchestrated by the anarchist activist group Anonymous (Infosecurity Magazine, 2011), also highlighted the potential danger of a reliance on cloud computing. What if your service provider is in some way implicated with a targeted organisation, or hosts services for sympathisers? I do not agree with the argument that security is improved just because small businesses do not have the in-house technical resources – they can outsource to a third party, and are probably already utilising a number of cloud based security solutions for email and web filtering (such as those provided by Webroot and Messagelabs/Symantec), email continuity, email encryption, online backup services, to name but a few. Reliability of broadband availability apart (and I am pretty sure this will continue to improve), from a business continuity perspective ubiquitous internet access to geographically dispersed information has its advantages. How many of us remember the Buncefield fuel depot fire in 2005 (Health and Safety Executive, 2005), when for many days, if not weeks, numerous small businesses were unable to gain access to their premises close to the depot and subsequently failed.

Depending on the service model adopted and how far down the delivery stack you go – whether it be SaaS, PaaS or IaaS – the greater the level of security risk and responsibility apportioned to you, the user. The higher up, the greater level of security emphasis placed with the service provider, although not necessarily accountability. It may come down to trust. As Bruce Schneier said in his blog (Schneier, A blog covering security and security technology, 2009):

“Trust is a concept as old as humanity, and the solutions are the same as they have always been. Be careful who you trust, be careful what you trust them with, and be careful how much you trust them. Outsourcing (Cloud Computing) is the future of computing. Eventually we'll get this right, but you don't want to be a casualty along the way”.

Tread very carefully.

Bibliography

- Amazon Web Services. (2010, November 9). *Amazon Cloudfront SLA*. Retrieved January 25, 2011, from Amazon Cloudfront: <http://aws.amazon.com/cloudfront/sla/>
- Amazon Web Services. (2010, August). *Amazon Web Services AWS Security Whitepaper*. Retrieved January 10, 2011, from Amazon Web Services: http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf
- Bloor Research. (2009, March 10). *EU Compliance and Regulations for the IT Professional*. Retrieved December 12, 2010, from Bloor Research: <http://www.bloorresearch.com/research/White-Paper/1025/eu-compliance-and-regulations-for-the-it-security-profession.html>
- Cloud Security Alliance. (2009, December). *Security Guidance*. Retrieved November 23, 2010, from Cloud Security Alliance: <http://www.cloudsecurityalliance.org/csaguide.pdf>
- Computer Weekly. (2004, April 5). *Fire in BT cable tunnel paralyzes Manchester business community*. Retrieved January 26, 2011, from computerweekly.com: <http://www.computerweekly.com/Articles/2004/04/06/201587/Fire-in-BT-cable-tunnel-paralyses-Manchester-business.htm>
- Financial Services Authority. (2008, April). *Data Security In Financial Services*. Retrieved December 14, 2010, from www.fsa.gov.uk: http://www.fsa.gov.uk/pubs/other/data_security.pdf
- Financial Services Authority. (2010, August 24). *FSA fines Zurich Insurance £2,275,000*. Retrieved December 14, 2010, from FSA Library: <http://www.fsa.gov.uk/pages/Library/Communication/PR/2010/134.shtml>
- Health and Safety Executive. (2005, December 11). *Buncefield Investigation*. Retrieved January 26, 2011, from Official site for the Buncefield Disaster Investigation: <http://www.buncefieldinvestigation.gov.uk/index.htm>
- Hulitzky, M. H. (2011). Business in the Cloud. In *What Every Business Needs To Know About Cloud Computing* (p. 30). Wiley.
- Information Commissioners Office. (2009). The Guide to Data Protection. In *How much do I need to know about Data Protection* (pp. 82-92). ICO.
- Infosecurity Magazine. (2011, January 25). *Anonymous hacking group uses IRC channels to coordinate DDoS attacks*. Retrieved January 25, 2011, from Infosecurity Magazine: <http://www.infosecurity-magazine.com/view/15393/anonymous-hacking-group-uses-irc-channels-to-coordinate-ddos-attacks/>
- Lacey, D. (2009). *Managing the Human Factor in Information Security*. Chichester: Wiley.

Microsoft. (2011, January 25). *Microsoft Office 365*. Retrieved January 25, 2011, from Microsoft: <http://office365.microsoft.com/en-US/online-services.aspx>

Murray, C. (2010, April 7). *Small businesses to be fined for security breaches*. Retrieved January 25, 2011, from SME Web - online resources for SMEs in the UK: <http://www.smeweb.com/content/view/2046/117/>

Office for National Statistics. (2010, September 27). *Analysis of UK businesses*. Retrieved January 25, 2011, from Office for National Statistics: <http://www.statistics.gov.uk/cci/nugget.asp?id=1238>

Page, C. (2010, March 11). *Two-day outage on Be in Beds/Herts*. Retrieved January 26, 2011, from broadbandbanter.com: <http://www.broadbandbanter.com/showthread.php?t=28911>

Schneier, B. (2009, June 4). *A blog covering security and security technology*. Retrieved December 18, 2010, from Schneier on Security: http://www.schneier.com/blog/archives/2009/06/cloud_computing.html

Schneier, B. (2010, December 16). *A blog covering security and security technology*. Retrieved January 11, 2011, from Schneier on Security: http://www.schneier.com/blog/archives/2010/12/security_in_202.html

Taleb, N. N. (2010). What you do not know. In N. N. Taleb, *The Black Swan* (p. prologue XXIII). Penguin Books.

The Economist. (2008, October 23). *A survey of corporate IT - Where the Cloud meets the Ground*. Retrieved January 3, 2011, from The Economist: http://www.economist.com/research/articlesbysubject/displaystory.cfm?subjectid=348981&story_id=E1_TNQTTJND

The Register. (2010, March 31). *Flood, fire at BT Paddington node causes widespread problems*. Retrieved January 14, 2011, from theregister.co.uk: http://www.theregister.co.uk/2010/03/31/burne_house_burns/

Vines, R. L. (2010). Cloud Security. In *A Comprehensive Guide to Secure Cloud Computing* (pp. 128-130). Wiley.

Appendix A

EU Compliance—Summary Comparison Table

Act	Geographic coverage	Industries and sectors affected	Scope of coverage notes
EU Data Retention Directive 2006/24/EC	EU	Telecoms	Data relating to electronic communications
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995	EU	All	Personal data
Capital Requirements Directive/Basel Accords	Global	Banking and Finance	Internationally-active banks with assets greater than \$250 billion or foreign exposures greater than \$10 billion
Payment Card Industry Data Security Standards (PCI DSS)	Global	All	Any that process card payments
The Rules Governing Medicinal Products in the European Union and Commission Directives 91/356/EEC, 2003/94/EC, and 91/412/EEC	EU	Pharmaceuticals	Computers used in the drug manufacturing process
MiFID - The Markets in Financial Instruments Directive	EU	Banking and Finance	Companies and banks trading in financial instruments and businesses that deal in advisory services
Statutory Audit and the Company Reporting Directives ("EuroSox")	EU – must be implemented into local laws by EU member states by 2010.	All	Public companies
Data Protection Act 1984, amended 1998	UK	All	Any organisation that collects personal data
Freedom of Information Act	UK (Scottish public authorities are subject to the Freedom of Information (Scotland) Act 2002)	Government bodies, local authorities and companies owned by the government	Information held by authorities, excluding personal data
Regulation of Investigatory Powers Act 2000 (RIP or RIPA) (UK)	UK	All	All electronic data
Federal Data Protection Act (November 2006) (Germany)	Germany	Public bodies of the Federation and the Länder. Private organisations and businesses	Private data held by these organisations
Freedom of Information Act (2005) (Germany)	Germany	Government and public bodies	Information held by authorities (excluding personal data)
Data Protection Act (2004) (France)	France	All	Any organisation that collects personal data
Law on Access to Administrative Documents (1978/2005) (France)	France	Government and public bodies	Information held by authorities (excluding certain data relating to national security issues etc.)
Control of Insurance Undertakings (1995) (Belgium)	Belgium	Insurance	Documents relating to contracts
Law of Privacy Protection (1998) (Belgium)	Belgium	All	Any organisation that collects any information relating to an identified or identifiable person
Money Laundering and Finance of Terrorism Law (1993) (Belgium)	Belgium	Banking	Documents and transaction records
Supervision of the Financial Sector Law (2003) (Belgium)			
Consumer Credit Law (1992) (Belgium)			

EU Compliance—Summary Comparison Table

Act	Geographic coverage	Industries and sectors affected	Scope of coverage notes
Personal Data Protection Act (2000) (Netherlands)	Netherlands	All	Any organisation that collects any information relating to an identified or identifiable person. Certain data categories are exempt.
Protection of persons with regard to the Processing of Personal Data (2002 and 2007) (Luxemburg)	Luxemburg	All	Any organisation that collects any information relating to an identified or identifiable person
Personal Data Protection Code (2004) (Italy)	Italy	All	Any organisation that collects any information relating to an identified or identifiable person. Includes deceased people
Civil Code section 2214 and 2220 (Italy)	Italy	All	All accounting records, emails, faxes, invoices and other business records
Protection of Personal Data (1999) (Spain)	Spain	All	Any organisation that collects any information relating to an identified or identifiable person.
Commercial Code (Spain)	Spain	All	All accounting and other business records
Personal Data Act (1999) (Finland)	Finland	All	Any organisation that collects any information relating to an identified or identifiable person. Indirectly covers the deceased if their sensitive data may affect living relatives
Personal Data Act (1998) (Sweden)	Sweden	All	Any organisation that collects any information relating to an identified or identifiable person
Accounting Act SFS 1999:1078 (Sweden)	Sweden	All	All companies
Public records Act SFS 1990:782 (Sweden)	Sweden	Government and public bodies	Public authorities and other bodies controlled by municipal bodies
EBICS - Electronic Banking Internet Communication Standard (Germany and France)	Germany and France	Banking and Finance	Organisations transmitting banking data
Government Code of Connection (CoCo) (UK)	UK	Government and Public Bodies	Organisations connecting to the Government Secure Extranet (GSX)
Payment Services Directive 2007/64/EC	EU	Financial Services	Businesses engaged in the processing of payment services

EU Compliance and Regulations for the IT Professional, Bloor Research November 2010

Amazon CloudFront Service Level Agreement (SLA)

Effective Date: November 9, 2010

This Amazon CloudFront Service Level Agreement (“SLA”) is a policy governing the use of the Amazon CloudFront under the terms of the Amazon Web Services Customer Agreement (the “AWS Agreement”) between Amazon Web Services, LLC (“AWS”, “us” or “we”) and users of AWS’ services (“you”). This SLA applies separately to each account using Amazon CloudFront. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement.

Service Commitment

AWS will use commercially reasonable efforts to make Amazon CloudFront available with a Monthly Uptime Percentage (defined below) of at least 99.9% during any monthly billing cycle (the “Service Commitment”). In the event Amazon CloudFront does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

Definitions

“Error Rate” means: (i) the total number of internal server errors returned by Amazon CloudFront divided by (ii) the total number of requests during that five minute period. We will calculate the Error Rate for each Amazon CloudFront account as a percentage for each five minute period in the monthly billing cycle. The calculation of the number of internal server errors will not include errors that arise directly or indirectly as a result of any of the Amazon CloudFront SLA Exclusions (as defined below).

“Monthly Uptime Percentage” is calculated by subtracting from 100% the average of the Error Rates from each five minute period in the monthly billing cycle.

A “Service Credit” is a dollar credit, calculated as set forth below, that we may credit back to an eligible Amazon CloudFront account.

Service Credits

Service Credits are calculated as a percentage of the total charges paid by you for Amazon CloudFront for the billing cycle in which the error occurred in accordance with the schedule below.

Monthly Uptime Percentage	Service Credit Percentage
Equal to or greater than 99% but less than 99.9%	10%
less than 99%	25%

We will apply any Service Credits only against future Amazon CloudFront payments otherwise due from you; provided that, we may issue the Service Credit to the credit card that you used to pay for Amazon CloudFront for the billing cycle in which the error occurred. Service Credits shall not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar (\$1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability or non-performance of Amazon CloudFront or other failure by us to provide Amazon CloudFront is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA or termination of your use of Amazon CloudFront.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a request by sending an e-mail message to aws-sla-request@amazon.com. To be eligible, the credit request must (i) include your account number in the subject of the e-mail message (the account number can be found at the top of the AWS Account Activity page); (ii) include, in the body of the e-mail, the dates and times of each incident of non-zero Error Rates that you claim to have experienced; (iii) include your server request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks); and (iv) be received by us within ten (10) business days after the end of the billing cycle in which the errors occurred. If the Monthly Uptime Percentage applicable to the month of such request is confirmed by us and is less than 99.9%, then we will issue the Service Credit to you within one billing cycle following the month in which the error occurred. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

Amazon CloudFront SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of Amazon CloudFront, or any other Amazon CloudFront performance issues: (i) that result from Service Suspensions described in Section 7.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon CloudFront; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (v) arising from our suspension and termination of your right to use Amazon CloudFront in accordance with the AWS Agreement; (vi) that result from

exceeding usage limits stated in the Amazon CloudFront documentation; or (vii) that result from use of an origin server other than Amazon S3 (collectively, the “Amazon CloudFront SLA Exclusions”). If availability is impacted by factors other than those used in our calculation of the Error Rate, we may issue a Service Credit considering such factors in our sole discretion.

(Amazon Web Services, 2010)