Communications of the IIMA

Volume 12 | Issue 4 Article 2

2012

The Conundrum of Security in Modern Cloud Computing

Thomas Sommer
Quinnipiac University

Tanya Nobile
Quinnipiac University

Paul Rozanski
Quinnipiac University

The Conundrum of Security in Modern Cloud Computing

Thomas Sommer
Quinnipiac University, CT, USA
thomas.sommer@quinnipiac.edu

Tanya Nobile
Quinnipiac University, CT, USA
tanya.nobile@quinnipiac.edu

Paul Rozanski
Quinnipiac University, CT, USA
paul.rozanski@quinnipiac.edu

ABSTRACT

In today's economic climate organizations are seeking greater cost-saving measures, increased agility, and scalability that responds to the rapid changes in technology and business. Cloud computing, with its low cost pay-as-you-go business model, is helping organizations manage these changes while transforming information technology (IT) into an engine that drives business. Benefits from on-demand clouds provide users greater portability and the ability to access information from virtually anywhere: at home, a client location, when traveling, or at the office. The reduced costs and increased flexibility, however, associated with cloud computing also come with complex security issues and increased overall risk. When cloud services are moved beyond organizational boundaries, outside the border firewall, security is heightened for most organizations and navigating the complexity of these environments can be daunting.

In this research paper we seek to help organizations make pragmatic decisions about where and when to use cloud solutions by outlining specific security issues that enterprises should address. We use external research sources and explore current security trends within cloud computing in order to provide background information, related research, and conclusions. We make use of colleagues, textbooks, peer reviewed journal articles, and Internet websites related to information technology and information security. Each section of our research is formatted similarly and presents pertinent security information, techniques, and tools that organizations would need in order to make relevant decisions when utilizing Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS).

Keywords: Security, cloud computing, trusted third party, cloud security, data privacy, network security, virtualization, SaaS, IaaS, PaaS

INTRODUCTION

In recent years many people have come to believe cloud computing is the most notable paradigm shift in information technology since the appearance of the Internet. According to industry analysts at Gartner Research, cloud technologies are now at the top of most CIOs' priority list and organizations are expediting their implementations of cloud services. Current estimates indicate that organizations are beginning to make the transition to this new model of computing and will collectively spend $148.8 billion worldwide on cloud services through 2016 (Gartner Research, 2010). As cloud computing quickly transforms the IT landscape, discussions regarding its adoption have progressed from **if** to **when**. Organizations of all sizes are now showing keen interest in cloud services that increase business agility and reduce technology infrastructure costs. Many cloud offerings provide both economic and strategic advantages, however they also present notable security risks for organizations that must defend against their intellectual property and corporate information assets, all while adhering to a variety of industry and government regulations (GeoTrust, 2011).

In spite of the economic rewards of using cloud computing, concerns about security risks and data privacy have slowed its adoption in many organizations (Gens, 2009). With so many different cloud deployment options, software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS); public vs. private deployments, internal vs. external hosting, and various hybrid configurations, all including virtualization, organizations need guidance and a framework that help them evaluate initial cloud risks and shape their security decisions. Additionally, over time as organizations expand from just one cloud service to using several from disparate providers, they must effectively manage these multiple cloud-service providers, with different infrastructures, operational practices, and security expertise. These levels of complexity require a pervasive and highly trustworthy method of securing organizational data as it is transported to and from cloud service providers.

BACKGROUND

The idea of cloud computing mystifies many managers and organizations. Similar terms are often used to describe cloud computing, such as: grid, distributed, on-demand, cluster, utility, virtualization, and software-as-a-service. More directly, cloud computing refers to end-users connecting with applications running on sets of shared servers, often hosted and virtualized, instead of a traditional dedicated server. For over thirty years client-server computing has provided applications that were assigned to specific hardware, often residing in on-premise data centers. On-demand cloud computing empowers its end-users by allowing them to use their choice of Internet-connected device, on any day or at any time (Knorr & Gruman, 2009).

The U.S. National Institute of Standards and Technology (NIST) describes cloud computing in their publication NIST 800-145, "The NIST Working Definition of Cloud Computing." NIST's definition describes five crucial characteristics (broad network access, rapid elasticity, measured service, on-demand self service, and resource pooling), three cloud service models (SaaS, PaaS, and IaaS), and four cloud deployment models (public, private, hybrid, and community), as seen in Figure 1 below (Cloud Security Alliance, 2011b).

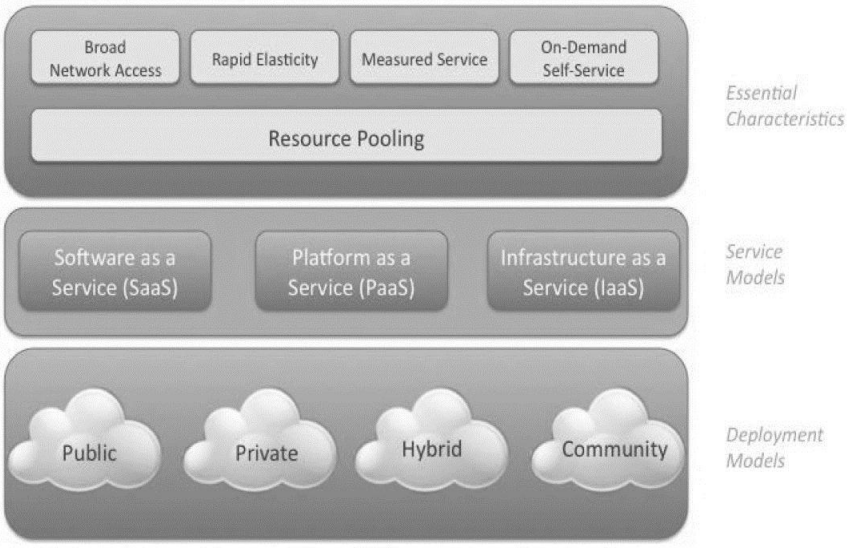

Figure 1: NIST Visual Model of Cloud Computing (Cloud Security Alliance, 2011b**).**

Service Models

Software-as-a-Service (SaaS), often referred to as on-demand software, is a software deployment and subscription-pricing model that delivers an enterprise application as a managed service by a software vendor. SaaS systems are accessible via the Internet, or a network, and are charged on a subscription service basis, often based on the number of users. SaaS solutions transfer the responsibility and liability of implementing and maintaining a system from the customer to the SaaS provider; thus eliminating additional costs and complexities when installing additional hardware, or hiring more support staff to fuel expansion and growth.

Infrastructure-as-a-Service (IaaS), often referred to as on-demand infrastructure, delivers computing infrastructure as a utility service, typically in a virtualized or multi-tenancy environment. IaaS users rent or buy servers, software, data-center space, network equipment, etc. as a fully outsourced service. IaaS often provides raw storage and networking with immense potential for extensibility and scale.

Platform-as-a-Service (PaaS) is a rich ecosystem for application development, programmer communities, and database development along with other applications as a solution stack or service. PaaS empowers application developers to build their own applications on top of the platform and often fill gaps in functional holes within a SaaS solution by facilitating deployment of applications without the cost and complexity of buying and managing the underlying hardware, server software, and provisioning or hosting capabilities. This provides all of the facilities required to support the complete software development life cycle (SDLC) whenever building and delivering web applications and services that are entirely available from the Internet (Cloud Security Alliance, 2011b).

From a security perspective there is key takeaway that the lower down the stack the cloud service provider stops, whether it be SaaS, IaaS, or PaaS, the more security the cloud consumer is

responsible for implementing and managing (Cloud Security Alliance, 2011b). Other key security takeaways for the three cloud service models are as follows:

- **SaaS** provides the most integrated functionality; however, the SaaS provider bears sole responsibility for security. SaaS is built upon IaaS and PaaS stacks and provides the entire user experience (content, presentation, applications) and all management capabilities.
- **PaaS** sits on top of IaaS and adds integration with application development frameworks, middleware, and other functions like database, messaging, and queuing. These services allow developers to build applications on the platform with programming languages and tools that are supported by the stack.
- **IaaS** resides under SaaS and PaaS, and provides a set of Application Programming Interfaces (APIs), which allow management and other interaction with infrastructure, along with vast extensibility.
- All cloud service models (SaaS, PaaS, and IaaS) should have strong, well-defined service level agreements (SLAs) that protect the cloud user with, according to the CSA, "service levels, security, governance, compliance, and liability expectations of the service and provider are contractually stipulated, managed to, and enforced" (Cloud Security Alliance, 2011b, p.16).

Deployment Models

Despite the service model (SaaS, PaaS, or IaaS) there are four deployment models for cloud computing services and variations of each:

- **Public Cloud** is owned by an organization selling cloud services and its infrastructure is made publically available to organizations, businesses, and industries.
- **Private Cloud** is managed by the organization or a third party and is either on or off premises. The cloud infrastructure is private, available to a single organization.
- **Hybrid Cloud** is managed by the organization or a third party and exists on or off premises. This cloud infrastructure combines two or more clouds (private, public, or community).
- **Community Cloud** is managed by the organization or a third party and exists on or off premises. This cloud infrastructure is shared by multiple organizations with common interests, requirements, or considerations (Grance & Jansen, 2011).

History and Future of the Field

In 1961, John McCarthy, a computer scientist and Stanford professor, spoke at MIT describing how future computer time-sharing, computing power, and applications could be sold and delivered as public utilities, such as electricity or water (Kopee, 2008). In 1969, researcher J.C.R. Licklider, who was responsible for enabling the development of ARPANET (Advanced Research Projects Agency Network), introduced the idea of an "intergalactic computer network" that would allow humankind to share data and information from anywhere in the world. Since McCarthy, the idea of cloud computing has evolved during the last 51 years, and in the 1990s the necessary bandwidth required to implement cloud computing became available at a large scale. In 1999, Salesforce.com began providing enterprise class software through its website, helping lay the foundation for future developers and application service providers. In 2002, Amazon Web Services began providing storage and computational services via its Amazon Mechanical Turk, and in 2006 expanded by releasing Amazon Elastic Compute Cloud (EC2) as a web service that

allowed large and small organizations (even individuals) to rent computer access on which anyone could run private applications. According to Brightcove's CEO, Jeremy Allaire, the "Amazon EC2 and Simple Storage Service (S3) was the first widely accessible cloud computing infrastructure service." Around this time the idea of browser based applications and Web 2.0 became even more popular when in 2009, companies like Google began offering collaboration suites, such as Google Apps, which were easily accessible from any Internet connected computer or mobile device (Mohamed, 2009).

Additional factors have helped the growth of cloud computing, including the evolution of virtualization technologies. According to Jamie Turner, a UK cloud computing pioneer, the development of broadband access, universal software standards, storage technologies, and especially virtualization have all helped create an environment where "cloud computing extends its reach beyond a handful of early-adopter Google Docs users;" and "we can only begin to imagine its scope and reach. Pretty much anything can be delivered from the cloud" (Mohamed, 2009).

As on-demand scalability of applications and resources, reduced infrastructure costs, increased storage capacity, and greater agility began helping organizations realize the benefits of cloud computing, many questions and concerns became widespread. The ideas of cloud security, trust, and data privacy, along with network performance, created apprehensiveness among cloud adopters (Mohamed, 2009). Cloud service providers responded with what the CEO of GFI Software, Walter Scott, called "extremes to protect their clients' data, rest assured that they are also using optimized mechanisms to replicate and secure that data across multiple disks, servers and locations" (Scott, 2010). Julian Friedman, an IBM Emerging Technology Specialist, believes cloud security and other concerns will be quickly resolved and adoption will expand, "considerations such as security, data privacy, network performance and economics are likely to lead to a mix of cloud computing centers both within the company firewall and outside of it" (Mohamed, 2009).

Aside from security and other concerns the future growth of cloud computing looks promising. Many analysts such as Gartner and Forrester Research agree and have begun forecasting their cloud taxonomy. In a popular 2011 report, analysts at Forrester Research provide keen insight into the future of cloud computing despite on-going security concerns including (Ried & Kisker, 2011):

- **SaaS** is forecasted to quickly become a catalyst of PaaS and IaaS growth, up to $132.5 billion market by 2020, representing 26% of all packaged software by 2016.
- **PaaS** is forecasted to grow to $11.91 billion market by 2020, and up to 15% of all corporate application development will be on this platform.
- **IaaS** is forecasted to experience rapid commoditization and then decline after 2014, consolidation will lead to $4.7 billion market by 2020 (Ried & Kisker, 2011).

David Linthicum (2011), IT strategist and adviser at Blue Mountain Labs, suggests the future of cloud computing beyond 2012 can be broken into three distinct categories, as described in Figure 2 below:

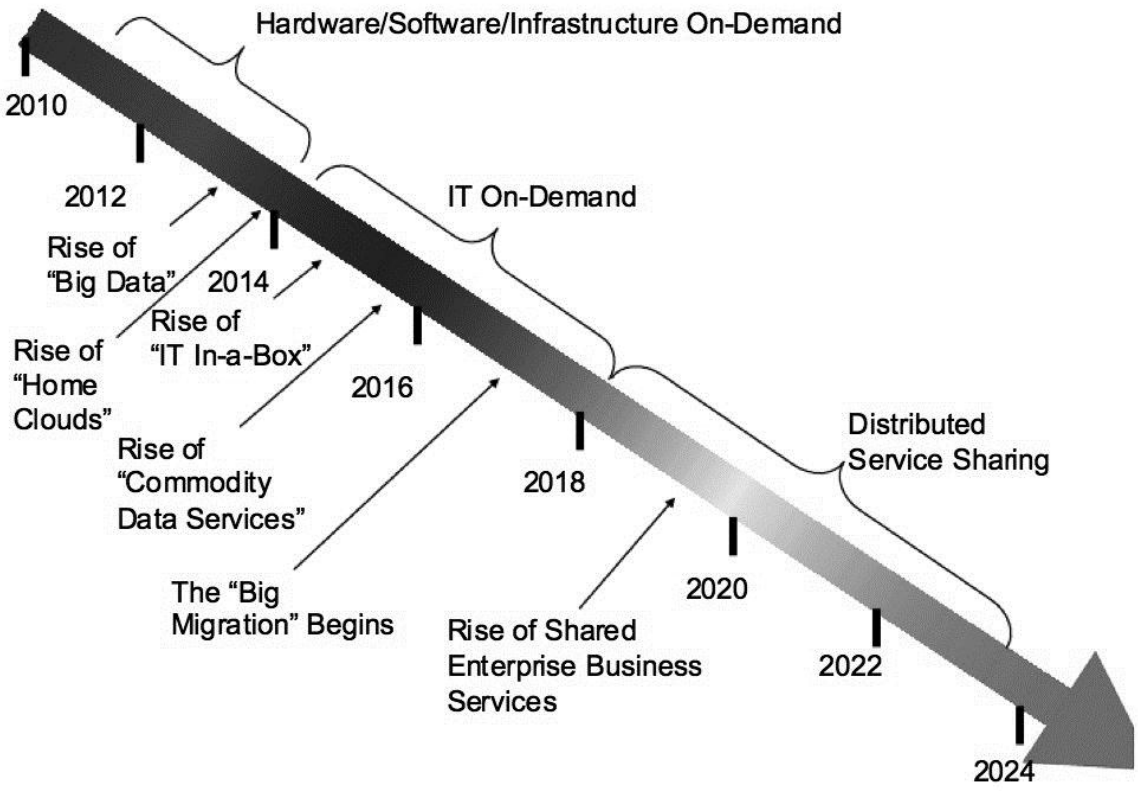

Figure 2: The Future of Cloud Computing (Linthicum, 2011).

Linthicum describes 2010-2014 as the era of on-demand hardware, software, and infrastructure due to increased demand for big data repositories and the need for personal (home) clouds. From 2014-2018 he believes IT on-demand will evolve as organizations seek to further leverage cloud deployments while commoditizing data services. From 2018-2024 Linthicum suggests cloud computing will provide distributed service sharing with organizations and enterprises sharing business services across global economies of various scale (Linthicum, 2011). The definitive future of cloud computing is yet to be determined; however, as with all computing evolutions there is risk and the threatscape surrounding the cloud will certainly evolve along with it.

The sheer scope and breadth of cloud services are rapidly expanding and evolving, as illustrated in the OpenCrowd Cloud Solutions taxonomy, Figure 3 below (OpenCrowd, 2012).

Cloud Controls and Top Threats

The Cloud Security Alliance (CSA) was formed by a coalition of industry practitioners and associations in 2008, as a not-for-profit organization, to promote the use of best practices for providing security assurance within cloud computing and all other forms of computing. The CSA suggests controls be implemented, "in one or more layers ranging from the facilities (physical security), to the network infrastructure (network security), to the IT systems (system security), all the way to the information and applications (application security)" (Cloud Security Alliance, 2011b).

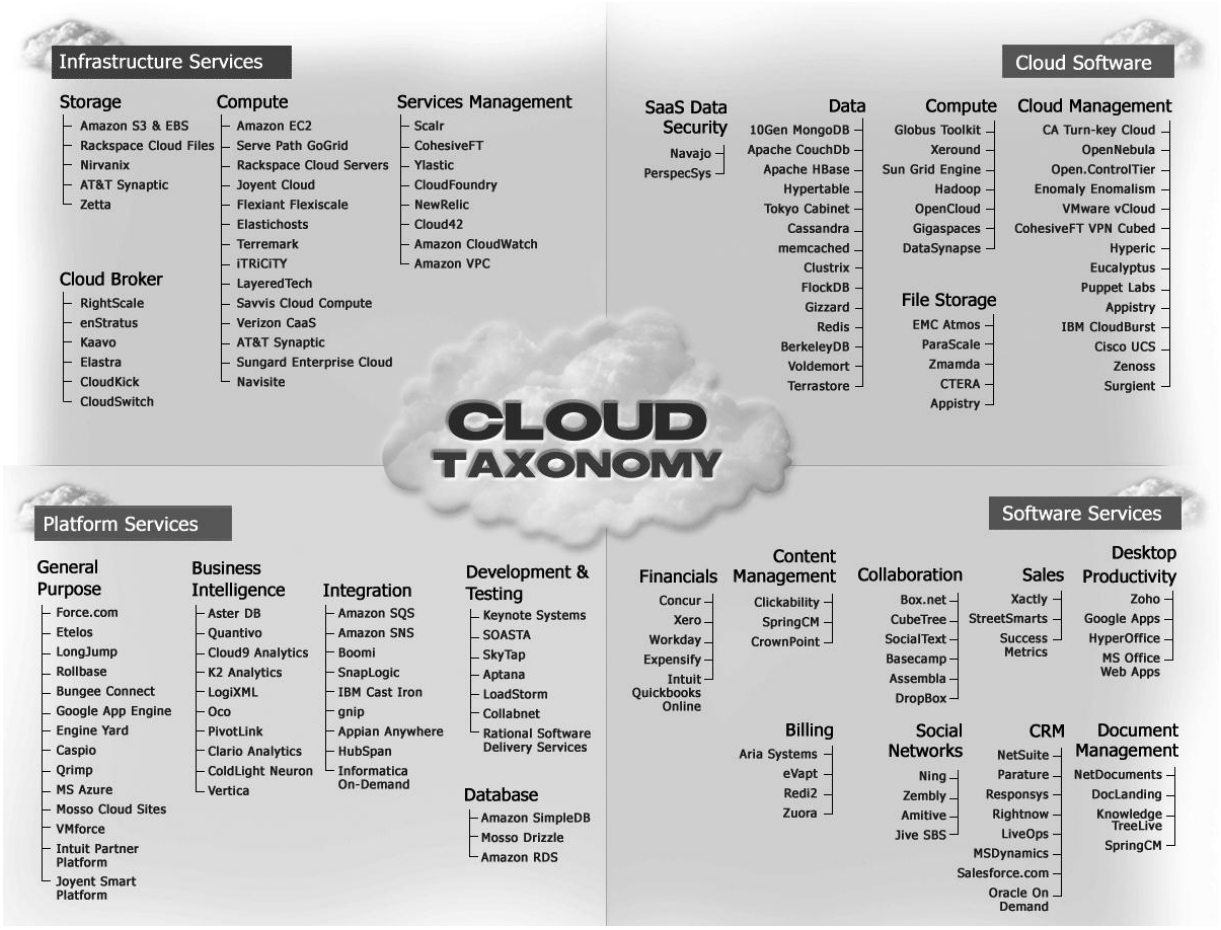

Figure 3: OpenCrowd Cloud Solutions Taxonomy (OpenCrowd, 2012).

The CSA describes risks and threats associated with cloud computing as unique, pertaining to the specific cloud service provider (CSP) and each should be rigorously evaluated using standard industry guidelines, such as The Open Group Architecture Framework (TOGAF), Sherwood Applied Business Security Architecture (SABSA), Information Technology Infrastructure Library (ITIL), Committee of Sponsoring Organizations (COSO), or Control Objectives for Information and Related Technology (COBIT). Additionally, the CSA provides guidance regarding top security concerns by creating 14 domains that all cover operating and governing cloud services. These domains emphasize security and privacy in a multitenant environment, for example: (Cloud Security Alliance, 2011b)

- Domain 1: Cloud Computing Architectural Framework
- Domain 2: Governance and Enterprise Risk Management
- Domain 3: Legal Issues: Contracts and Electronic Discovery
- Domain 4: Compliance and Audit Management
- Domain 5: Information Management and Data Security
- Domain 6: Interoperability and Portability
- Domain 7: Traditional Security, Business Continuity, and Disaster Recovery
- Domain 8: Data Center Operations
- Domain 9: Incident Response

- Domain 10: Application Security
- Domain 11: Encryption and Key Management
- Domain 12: Identity, Entitlement, and Access Management
- Domain 13: Virtualization
- Domain 14: Security as a Service (Cloud Security Alliance, 2011b)

IT security experts have also identified specific security challenges related to cloud computing. According to Bob Violino, of CSOonline.com, five major cloud security issues currently exist: smartphone data slinging-users accessing large amounts of data on mobile devices, better access control and identity management across multiple clouds, ongoing compliance concerns, the risks of multiple cloud tenants, and the emergence of cloud standards and certifications (Violino, 2010).

Another CSOonline.com investigator, Mary Brandel, described additional cloud security issues within the various cloud models and how they plague real world adoption of cloud services. In the SaaS cloud model security concerns regarding single sign-on authentication and the need to integrate with Microsoft's Active Directory present real difficulties. In the IaaS cloud model security concerns with data encryption, virtualization, business continuity, and auditing all introduced significant problems. Furthermore, in the on-site private cloud model additional security concerns existed regarding virtualization in multitier infrastructures and the implementation of virtual firewalls (Brandel, 2010).

Cloud computing is also threatened by several new security scenarios, along with new evolutions of threat vectors, according to McAfee's 2012 Threats Predictions Report. These security threats will impact cloud computing and all other types of computing regardless of delivery model, according to McAfee, and should therefore be addressed as such. These significant threats McAfee identified include: industrial threats that will mature and segment, embedded hardware attacks, Hacktivism from organizations like Anonymous, virtual currency systems attacks, ongoing Cyberwar, new DNSSEC network threat vectors, spearphishing targeted messaging attacks, mobile botnets and rootkits, rogue certificates and rogue certificate authorities, and next-generation operating system botnets and rootkits (McAfee Labs, 2012).

According to a recent 2012 survey conducted by CIO.com, at least 82% of U.S. companies trust cloud computing enough to use it in some deployments. Although of those surveyed, 54% also believe cloud security is a high priority. When asked how IT professionals are securing their cloud servers 31% said their cloud service provider does it for them, while 21% provide security themselves manually using a checklist (Olavsrud and Muse, 2012). Regardless of the popularity of cloud computing or the method in which security professionals choose to secure these services, some serious threats have impacted organizations using the cloud. Some of these well-publicized threats have affected not only information security and data integrity, as well as privacy, governance, and in some cases regulatory compliance. In their 2012 Security Threat Report, security experts at Sophos outlined some of the largest cloud security breaches of 2011 (Sophos, 2012b).

- **DropBox**. Researchers discovered 45 million cloud file sharing users could be hacked in three different ways without authorization, by simply typing the account email address.

- **Epsilon**. This bulk email marketing company disclosed privacy information, including names and email addresses, of millions of customers from Chase Bank, Best Buy, Marriott, and Walgreens.
- **Sony**. The PlayStation Network encountered multiple breaches, risking 100 million customer accounts, possibly making this the most expensive data breach ever—costing up to $2 billion.
- **Stratfor**. Hacktivist organization Anonymous breached servers at this subscription-based provider of geopolitical analysis. Data was stolen including 75,000 credit card numbers, 860,000 user names and passwords, and later Anonymous revealed this private information on the Internet.
- **Social Networks**. Several attacks on popular social networks have been successful, including: defacement of Microsoft's and *Sesame Street's* YouTube channels, Pfizer's Facebook page, and Twitter accounts of both NBC News and USA Today (Sophos, 2012b).

Other threats have been identified and are constantly evolving at alarming rates. In fact, according to Sophos and Angelo Comazzetto, Senior Product Manager, "A new web threat is detected every 4.5 seconds." And a "dark side of cloud computing are botnets." Comazzetto argues that botnets present a real-time threat and cloud service providers should use security gateways that offer comprehensive unified threat management (UTM) (Comazzetto, 2012).

Recently Marco Balduzzi, a senior threat researcher for Trend Micro, presented a Black Hat sponsored webcast where he illustrated significant privacy and security risks associated with renting and using public Amazon Machine Images (AMIs) from cloud computing providers. Dr. Balduzzi argued that IBM SmartCloud and Amazon's EC2 allow users to create and share virtual images that have been improperly and insecurely preconfigured. His extensive security research involved both local and remote testing, using various tools such as NMAP, Nessus, and SatanCloud, and lasted 7 months—involving over 5,000 Linux and Windows AMIs. Balduzzi found that 98% of Windows and 58% of Linux AMIs come with critical vulnerabilities including: unsolicited connections, various malware, leftover credentials, privacy risks, forgotten cryptography keys, and others (Balduzzi, 2012). The key takeaways from this research involved the need for much better due diligence when using cloud computing, including:

- Immediately update all software, with the firewall running
- Regenerate the SSH host key, delete all others (users, passwords, or SSH keys)
- Check all configuration files of any services needed to run
- Check all suspicious connections, both outgoing and incoming
- Do not use public cloud images, prepare images yourself (Balduzzi, 2012)

During the same Black Hat sponsored webcast on cloud security, Vice President and General Manager of Mykonos Software, David Koretz indicated that 70% of all threats are against the web application layer and 73% of organizations have been hacked in recent two years due to insecure web applications, based upon independent research from Gartner and the Ponemon Institute. Koretz stated that SaaS and PaaS users should use advanced deception-based cyber-security, like Mykonos, to protect websites and web apps (Koretz, 2012).

While some security professionals view cloud security with skepticism, others still believe the cloud can actually make data safer. Ed Amoroso, chief security officer at AT&T, believes the,

"shift to cloud architecture can improve on current security practices by moving computing power and application intelligence to a centralized complex of servers, accessible via light clients." According to Amoroso, cloud computing is similar to mainframe era prior to early 1990s which did not require end-user software patches and is therefore less likely to have targeted malware. Amoroso suggests cloud computing is, "superior to what we have today," because the cloud also provides substantial security by taking away non-diverse devices from the computing environments and by providing multiply security layers, e.g. security of the underlying infrastructure combined with identity management (Amoroso, 2011).

Additionally, by using cloud computing for remote access, organizations are no longer using insecure methods, such as Symantec's pcAnywhere. Instead they are migrating to cloud-enabled services or virtual desktop infrastructure, according to Robert Lemos, Contributing Editor at Dark Reading. Vice President of Engineering and Operations for Citrix Online, Malte Muenke, believes "one of the fundamental benefits of cloud is the reduction of the attack surface—there are no open ports," and no inbound connections to a host computer because a host pulls data down from a cloud service. This results in a reduced attack surface that is centrally managed and can be more easily secured and/or monitored (Lemos, 2012a).

Security Certifications, Standards & Inspections

Many cloud security standards are being developed including those by: the IBM-backed Cloud Standards Customer Council (CSCC); the Open Data Center Alliance (ODCA), an Intel-backed standards organization formed last year, which includes BMW, Deutsche Bank, JPMorgan Chase, Marriott International, Shell and Disney Internet Labs; and as previously discussed, the Cloud Security Alliance (CSA) backed by Coca-Cola and eBay (Thibodeau, 2011). These organizations are actively developing comprehensive security standards for cloud service providers (CSPs), some of which are:

- **HIPAA and FINRA** guidelines provide assurance for financial services and health care organizations
- **Safe Harbor Compliance** is designed to prevent accidental information disclosure or loss
- **FIPS 200 / SP 800-53** defines 17 security requirements in areas that include access control, configuration management, contingency planning, identification and authentication, incident response, and system and information integrity. FIPS 200 also mandates the use of SP 800-53, to provide guidelines for selecting and specifying security controls.
- **ISO 27001 & 27002** provides 33 information security controls for evaluating, implementing, maintaining and improving an information system management system. Useful for multinational organizations.
- **SSAE 16** recently replaced SAS70, issued by American Institute of Certified Public Accountants (AICPA)
- **SOC 2 & 3** auditor reports that provide detailed descriptions of tests, results and levels of trust (Trappler, 2011).
- **WebTrust and SysTrust**, developed by the Canadian AICPA/CICA, a family of assurance services that are used by practitioners in the performance of Trust Services that include: security, availability, processing integrity, confidentiality, and privacy (WebTrust, 2012).
- **Certificate of Cloud Security Knowledge (CCSK)** recently developed by the Cloud Security Alliance is the industry's first user certification program for secure cloud

computing. It covers best practices outlined by the CSA and the European Network and Information Security Agency (ENISA) (Cloud Security Alliance, 2012a).

The United States has joined this process by launching the Federal Risk and Authorization Management Program (FedRAMP), a cloud security standards program that requires federal agencies to use cloud service providers who meet these standards. Federal CIO VanRoekel said that FedRAMP creates a "do once, use many times" framework that covers SaaS, PaaS and IaaS along with security assessments, authorizations and on-going monitoring (Vijayan, 2011).

Cloud computing and its service providers require the management of various classes and relationships, all within the context of comprehensive security controls. How clouds will be deployed and their consumption model is key. Whether they are on- or off-premise locations, as well as the types of resources, assets, and information being managed, all weigh heavily on the appropriate decision as to who manages them and how. Additionally, security controls must be selected and integrated in order to meet current and future compliance objectives (Cloud Security Alliance, 2011a). In this section we review some of the work being done in cloud security by both cloud service providers (CSPs) and related security professionals.

Cloud Security Techniques and Tools

At the recent RSA Conference in San Francisco during February 2012, a panel of security experts at the Cloud Security Alliance (CSA) Summit discussed how cloud computing's future security depends largely on mobile computing. As organizations move their infrastructures to cloud models their data is being accessed from anywhere in the world and passwords are a major weakness for cloud providers. These same industry experts agreed that in the future mobile computing should provide the preferred authentication platform to most users. Furthermore, too often employees' access corporate networks using unprotected or compromised mobile devices, these bring-your-own-devices (BYOD) represent significant hurdles for organizations because they commonly have inadequate controls in place that are managed by IT professionals (Lemos, 2012b).

Organizations of all sizes have difficult decisions to make when determining the appropriate level of security and the right cloud solution. A cloud migration process requires the use of various techniques and implementation tools, most of which are provided by cloud providers, such as Amazon. According to analysts at BMC Software, the key steps to successful cloud design and planning include:

- **Cloud Operations Definition** defines the cloud architecture, diagrams required performance and capacity, and determines operational compliance and security requirements.
- **Cloud Business Planning** determines business needs, current and future demands, management of the cloud service provider, service and contract pricing, and guarantees regulatory compliance.
- **Cloud Service Design** is designed to meet organizational needs by creating a service catalogue of critical services offered within the cloud-based system. Often these services are made up of: resource configurations (including hardware and storage), operating systems, applications, networking options, compliance packages, monitoring tools, service level agreements (SLA), and pricing of various components. (BMC Software, 2011)

As organizations evaluate cloud solutions they should carefully examine their overall risk, and identify critical security controls before they determine their preferred cloud solution. Sanjeev Aggarwal and Laurie McCabe, partners at Hurwitz & Associates, believe organizations should specify any **must-have** functionality and their requirements for real-time data visibility and security. Application interaction and reporting should be considered along with security issues related to internal resources that are needed to implement and manage the cloud service or system. Scalability should be automatic whenever needed and therefore future growth must be considered. Ease of access and mobile use of the cloud should be determined. Communication and collaboration abilities within the cloud services must be ascertained. The security issues related to modifying and adding new functionality should be considered in preparation for future growth. Multi-tenancy, or the capacity to share a single instance of the cloud software while serving multiple organizations but keeping data private, should be examined along its levels of security. Finally, global support and service should be clarified to determine how the cloud service provider tracks and manages system problems at the local, regional or country levels (Aggarwal & McCabe, 2011).

Organizations that plan to manage private, on-premise cloud services also have their own security challenges. Fortunately, several cloud security specialists, such as Sophos and McAfee, are now offering solutions that aid in data loss prevention. Sophos offers SafeGuard Enterprise Encryption for Cloud Storage, a solution that allows users to automatically and invisibly encrypt files uploaded to cloud storage services like Dropbox or Microsoft's Skydrive. SafeGuard provides centralized key management and uses FIPS 140-2 validated cryptography, AES 256 bit symmetrical encryption, and PKCS #5 password hashing (Sophos, 2012a). Additionally McAfee offers a Cloud Security Platform that can be deployed as an on-premise appliance, in a SaaS model, or in hybrid combinations. McAfee's products include: identity management, Data Loss Prevention (DLP) with virtual machine support, both email and web gateways, and a services gateway—all available within an electronic policy manager that provides configurability, monitoring, and security event visibility (Eddy, 2011).

When implementing private, public or hybrid clouds, organizations need criteria that help them assess cloud security, and determine control objectives; along with criteria that use established standards and best practices to all meet compliance requirements. The Cloud Security Alliance Cloud Controls Matrix (CCM) provides these underlying security principles as part of its governance, risk management and compliance (GRC) stack. The CSA's CCM helps guide cloud service providers and their customers in evaluating the total security risk of a particular cloud provider. According to CSA its CCM is a "customized relationship to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP and will augment or provide internal control direction for SAS 70 attestations provided by cloud providers" (Cloud Security Alliance, 2012b).

SecaaS: Security-as-a-Service

In 2011 an Intel IT Center survey on cloud security indicated at least 64% of IT decision makers surveyed are influenced by the best practices and standards established by the Cloud Security Alliance (CSA). Additionally, the remainder sought guidance from the Open Data Center Alliance (ODCA), the Trusted Computing Group (TCG), and the Distributed Management Task Force (DMTF) (Intel IT Center, 2011).

IT decision makers and potential customers are concerned about the security risks of cloud computing and, more directly, the forfeiture of control over systems they must secure. Cloud service providers (CSPs) traditionally offer security services however, according to the Cloud Security Alliance, "these services take many forms, they have caused market confusion and complicated the selection process." In order to help both cloud computing providers and their customers the CSA, in 2011, began a research project to "provide greater clarity on the area of Security as a Service" which will "enable enterprises to make use of security services in new ways, or in ways that would not be cost effective if provisioned locally" (Cloud Security Alliance, 2011a, p.7). SecaaS has the potential to address several cloud vulnerabilities, such as: IDS, virus protection, logging, identity management, cryptography, and many other cloud vulnerabilities (Carvalhoh, 2011). SecaaS categories include: (Cloud Security Alliance, 2011a)

- **Identity and Access Management (IAM)** provides controls for assured identities and access management. This category is both protective and preventative.
- **Data Loss Prevention** provides monitoring, protection, and verification of both on-premises and cloud data. This category is preventative.
- **Web Security** provides real-time protection, either on-premise using software or appliance or by proxying or redirecting traffic to a cloud service provider. This category is protective, detective, and reactive.
- **Email Security** provides control over email (inbound and outbound), protects organizations from phishing, malicious attachments, enforces acceptable use and spam policies, and provides business continuity options. This category is protective, detective, and reactive.
- **Security Assessments** provides third-party audits or assessments, based on industry standards. This category is detective.
- **Intrusion Management** provides pattern recognition in order to detect or react to unusual events, includes real time to blockage or prevention of an intrusion. This category is detective, protective, and reactive.
- **Security Information and Event Management (SIEM)** provides real-time reporting and alerting, event logging information by either push or pull device, and prevents tampering of evidence for future investigation. This category is detective.
- **Encryption** provides encryption using cryptographic algorithms. This category is protective.
- **Business Continuity and Disaster Recovery** provides mechanisms that are planned and implemented with operational resiliency in case of service interruption. This category is reactive, protective, and detective.
- **Network Security** provides security services that protect and dispense underlying resources and services. This category is detective, protective, and reactive (Cloud Security Alliance, 2011a).

DISCUSSION

Organizational and Managerial Issues

As organizations look for "increased productivity, agility, scalability and reliability, as well as reduced operating costs" (Hawes, 2012, p. 4), today's IT leaders are faced with wading through a variety of cloud computer deployment options. They must balance the cost, security, and

integrity of their systems, with a driving business demand. In their report, *Five Cloud Computing Trends That Will Affect Your Strategy Through 2015,* Gartner Analysts list cloud computing as one of the top 10 strategic technology trends that IT professionals will be addressing. They go on to describe cloud computing services not only as "service-based, elastically scalable, use shared resources, can be metered by use and use Internet technologies" (Cearley & Smith, 2012, p. 2); but also as a "style of computing that is applied to the creation, deployment, access and management of internal infrastructure and service" (Cearley & Smith, 2012, p. 2).

The 2011 Future of Cloud Computing Survey Results from the survey conducted by GigaOM Pro supports cloud technology as an increasing trend. "GiagOM Pro research conducted in 2011 found that 64 percent of businesses surveyed were experimenting with or using in production, cloud computing technologies" (Hawes, 2012, p. 4).

Additionally, the Gartner Analyst report *Predict 2012: Cloud Computing Is Becoming a Reality*, states; "Lured by the anticipated immediate benefits of the cloud as a platform…many organizations are determined to include the cloud in their planning for IT modernization" (p. 4). CIOs need to think of Cloud offerings as a tool in their tool-box to be used in support of overall technology strategy. What makes this so difficult is the belief that "there are no ensured success patterns, no standards, no best practices and no established long-term leaders" (Smith et al., 2011).

Security and Privacy Issues from a Business Perspective

With the excitement and allure of Cloud computing, there is also a degree of concern about the security and privacy issues. CIOs are accountable for their systems and data, however, they lose direct control over them when using cloud computing. Without controls in place guiding the appropriate level and form of security testing for cloud providers, this is a very real concern for organizations and IT alike. "Cloud vendors of all kinds – including providers of application operations, data management, infrastructure management and security – will become targets for hackers worldwide. This is because cloud providers store critical data from a large number of clients" (Smith et al., 2001, p. 8). When considering the benefits of cloud computing, organizations need to evaluate cloud services for their ability to resist security threats and attacks. "Enterprises will be unable to test cloud providers' systems themselves, because the applications or software that the cloud provider uses to service its cloud clients are unavailable to its enterprise clients for testing" (Smith et al., 2001, p. 8). The article, Addressing Cloud Computing Security Issues, categorizes these threats as data control, management console security, malicious insiders, account control, and multi-tenancy issues (Zissis & Lekkas, 2012).

This is in alignment with the Cloud Security Alliance's (CSA) report *Top Threats to Cloud Computing V1.0*. CSA lists insecure interfaces and APIs, malicious insiders, shared technology issues, data loss or leakage, account or service hijacking, unknown risk profile, and abuse and nefarious use of cloud computing, as the top security issues surrounding cloud computing.

When connecting to the cloud, data traffic between the organization and the cloud travels over the public Internet. This opens the opportunity for traffic to be compromised. "Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact

with cloud services" (Cloud Security Alliance, 2010, p. 9). A client may be exposed to attacks such as SQL injection, cross-site scripting, and cross-site request forgery if the interfaces that service the cloud's clients are weak.

When using cloud services, you are opening up the organization to attacks from malicious insiders who are part of the cloud services' vendor. Companies need to rely on that vendor's hiring practices, standards, security and screening policies. "A provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance" (Cloud Security Alliance, 2010, p. 10). The employees of the cloud service vendor may have broad access to the organization's data including private or sensitive data. The cloud vendor may have insufficient authentication, authorization and audit controls in place to protect the data. A data breach can result not only in damage to the organization's reputation, but also have legal ramifications and prompt compliance violations. Forrester analysts warn that few cloud providers assure protection for data being used within the application or for disposing of your data (Rapport, 2011). It is essential that organizations understand what the cloud provider is accepting responsibility for and that data must be secured, not only in transit between your organization and the provider, but also when it is on their servers and being accessed by cloud-based applications.

Additionally, not only are you sharing your company's data with the cloud vendor, you may also be sharing infrastructure with other organizations. Although hypervisors are employed to create virtual containers within the shared infrastructure, this is a security concern. "Hypervisors have exhibited flaws that have enabled guest operating systems to gain in appropriate levels of control or influence on the underlying platform" (Cloud Security Alliance, 2010, p. 11). Customers should not have access to each other's data, traffic, logs, etc.; however, you do not always know with whom you may be sharing the infrastructure. "Cloud computing is based on a business model in which resources are shared (i.e., multiple users use the same resource) at the network level, host level, and application level" (Zissis & Lellas, 2012, p. 586).

Legal and International Issues

The adoption of cloud computing can also introduce additional legal concerns. Gartner Analysts comments "you need to be aware of the local regulations and data privacy restrictions of the country where your cloud provider operates its business and the country where your cloud provider keeps its computing infrastructure and data centers" (Smith et al., 2001, p. 3). One of the basic tenets of cloud computing is the ability for data to be stored on the service provider's server instead of the organization's server. The service provider's servers can be located in Europe, Asia, the United States, or anywhere else. "This tenet of cloud computing conflicts with various legal requirements, such as European laws that require an organization know where the personal data in its possession is at all times" (Zissis & Lekkas, 2012, p. 586). Many countries throughout the world have different laws and regulations impacting the privacy of personal data. Cloud Security Alliance (CSA), Security Guide V3.0 provides the following examples of legal issues pertaining to personal data in the cloud, which companies need to be aware of described in Table 1 below (Cloud Security Alliance, 2011b. pp. 36-37)

Issue	Description
U.S. Federal Laws	Numerous federal laws and their related regulations, such as GLBA, HIPAA, Children's Online Privacy Protection Act of 1998 (COPPA), together with orders issued by the FTC, require companies to adopt specific privacy and security measures when processing data, to require similar precautions in their contracts with the third party service provider.
U.S. State Laws	Numerous state laws also create an obligation on companies to provide adequate security for personal data and to require their service providers to do the same. State laws that address information security issues generally require, at a minimum, that the company have a written contract with the service provider with reasonable security measures. See for example the extensive requirements under the Massachusetts Security Regulations.
Standards	Standards such as PCI DSS or ISO 27001 also create a domino effect similar to that of federal and state laws. Companies that are subject to PCI DSS or ISO 27001 must both comply with specified standards and pass onto their subcontractors the same obligation to meet the standard to which they are subject.
International Regulations	Many countries have adopted data protection laws that follow the European Union model, the OECD model or the APEC model. Under these laws, the data controller (typically the entity that has the primary relationship with an individual) remains responsible for the collection and processing of personal data, even when third parties process the data. The data controller is required to ensure that any third party processing personal data on its behalf takes adequate technical and organizational security measures to safeguard the data.
Contractual Obligations	Even if a specific activity is not regulated, companies may have a contractual obligation to protect the personal information of their clients, contacts or employees, to ensure that the data are not used for secondary uses, and are not disclosed to third parties. This obligation may stem, for example, from the Terms and Conditions and Privacy Statement that a company post on its website. Alternately, the company may have entered into contracts (such as service agreements) with its customers, in which it has made specific commitments to protect the data (personal data or company data), limit their use, ensure their security, use encryption, etc. The organization must ensure that, when data in its custody are hosted in the cloud, it will have the continued ability to meet the promises and commitments that it made in its privacy notice(s) or other contracts.
Prohibition against cross border transfers	Many laws, throughout the world, prohibit or restrict the transfer of information out of the country. In most cases, the transfer is permitted only if the country to which the data are transferred offers an adequate protection of personal information and privacy rights. The purpose of this adequacy requirement is to ensure that the individual data subjects whose data are transferred across borders will be able to enjoy, in the new country where their data were transferred, privacy rights and privacy protections that are similar to, and not less than, those that were afforded to them before the transfer. Thus, it is important for a cloud user to know where the personal data of its employees, clients, and others will be located, so that it can address the specific restrictions that foreign data protection laws may impose. Depending on the country, the requirements for ensuring this adequate protection may be complex and stringent. In some cases, it may be necessary to obtain prior permission of the local Data Protection Commissioner.

Table 1: Security Guidance for Critical Areas of Focus in Cloud Computing v3 (Cloud Security Alliance, 2011b, p 36-37.

In addition to these laws and regulations, moving data to a cloud environment creates somewhat unclear territory when it comes to defining who has possession, custody and control of the data especially when it comes to e-discovery. For example, in most of the United States a party is only obligated to produce documents that are within their possession, custody, or control.

Moving data to a hosted environment does not remove that obligation; however, not all clients' data may be accessible within a cloud configuration. The cloud provider may have control of some of the data, such as log files.

"The cloud is a worldwide phenomenon, and, in theory, it has no national boarders" (Smith et al., 2011, p. 3). Organizations need to understand this theory as well as the legal ramifications of it when entering into agreements with cloud providers. Companies must do due diligence in evaluating the legal ramification of their agreement. These legal issues around regulations and privacy rules have slowed the adoption of cloud computing in Europe. Gartner Analysts predicts that cloud adoption to be delayed by at least two years. "Despite a few decades of pan-European policies to facilitate the exchange of goods and services among European countries, and a still partial . . . single currency, many local regulations . . . and several restrictions on the flow of cloud data among countries are still very much in place, and are unlikely to go away in the short term" (Smith et al., 2011, p. 3).

The future of cloud computing security will directly relate to a combination of many significant aspects. According to Moore's Law, technology doubles every two years. The ability of security standards to continually grow and adapt to the security threats present will be the main focus of cloud computing security. Rake Narang, Editor-in-Chief of *Info Security Products Guide*, has compiled a small list of the top five data security concerns (Parann-Nissany, 2012). The list is as follows:

- **High Security** maintains that basic security essentials must be in place to create organizational trust. Security and trust go hand-in-hand, as there is always human intervention at some point in the system. The ability to create this trust is a concern for generations within a cloud computing security system.
- **Regulatory Compliance** means that complying with standards is a must for cloud computing security; thus providing consistency and uniformity with specific security measures.
- **Flexible Deployment and Provisioning** is one of the most important stages of cloud computing security implementation is the deployment and provisioning stage. The ability of a vendor to provide flexibility without compromising security is a significant concern for customers that must be addressed prior to implementation.
- **Dealing with complexity** is a challenge and constantly changing threat as a whole. The ability of complex security threat to conform and change is a major concern in the future. If security threat complexity is not a main focus, overall cloud security can easily show signs of weakness.
- **Effective Key Management** provides encryption that has transformed into a severely complex nature. There always has, and always will be potential security threats when the use of keys are involved in a security system. Key splitting and homomorphism technologies are solutions that can help resolve this challenge (Parann-Nissany, 2012).

These 5 key components must be addressed in order for cloud computing security to survive both current and future threats. Management is a key survival factor when using cloud computing. Without proper management and planning, the potential for security risks increase, and the overall security of an organization's system can easily be compromised. Attention to detail and proper control of the system must be addressed as a main focus of design and implementation.

Organizations that plan to migrate to cloud computing must not only plan for the present implementation, but also for the future. Linthicum (2011) addressed five key trends for the future of cloud computing at the recent Cloud Expo. The first trend is the potential removal of the word **cloud** from the term **cloud computing**. He believes cloud computing will eventually become the norm; and therefore be referred to simply as **computing**. The second trend is the emergence of focus on functionality, as opposed to the popularity due to hype. Cloud computing, as a whole, has not nearly reached the limits in which it can provide a positive and secure method of data storage for organizations of any type or size. Linthicum feels as though it will take a few years for cloud computing to be used comfortably. Third, the management of cloud computing will likely take on a more central position. Once trust and security are at a significantly strong point within cloud computing, the possibilities will be endless. This in turn will create more complexity within systems, another issue and concern for both users and vendors. The fourth trend is simply using the centralized data to gain a key strategic advantage, both in quantity and quality. The more information available, the better a system can function and operate. The ability to obtain valuable information both quickly and securely is one of the strongest attractions of cloud computing. The final trend anticipated by Linthicum is the application and growth of cloud computing through the use of mobile devices. With the continued rise of mobile computing and the reliance on clouds to support their applications, mobile devices will have more capabilities, but the data will live in the cloud (Linthicum, 2011). These trends are only a few of the many that will surely gain visibility in the near future for cloud computing. The continued popularity and development of cloud security measures and standards will play a major role in determining the future use of cloud computing within organizations.

Cloud computing security has grown substantially over the past decade. In order to survive, critical techniques and standards are forced to fluctuate and reform as a tactic to mitigate potential security threats and risks. With security being the number one concern for storage of important data, focusing on the security standards and how they are to be implemented becomes a major factor for both customers and vendors. Below is a chart displaying seven known security risks in cloud computing according to a new study from the Ponemon Institute (Vizard, 2010).

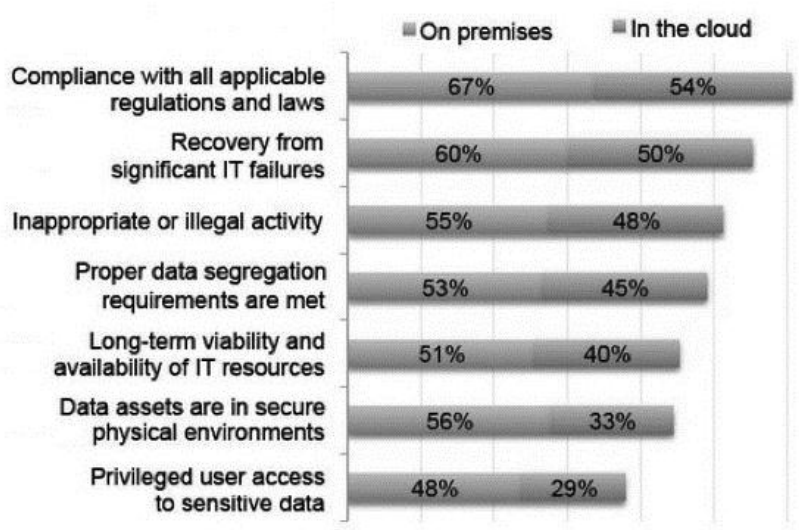

Figure 4: Seven Security Risks in Cloud Computing Environments (Vizard, 2010).

This chart compares the risks both on the premises and in the cloud, and serves as visualization of how much greater the risks are on premises as opposed to in the cloud; as well as a testament to the significant, positive results that cloud computing offers. Larry Ponemon, chairman of the Ponemon Institute, says the study clearly shows that, at the moment, the risk factors with cloud computing are high because not all cloud service providers have the same level of security. In addition, there is no security rating system in place for cloud computing, so cloud users cannot even rely on third-party security validations (Vizard, 2010). As the amount of data within the cloud grows, the risks increase as well. Cloud data will continue to reach new highs in both quantity and quality. Security standards are continually adapting and creating a more secure cloud environment. As a result, this facilitates a positive increase in quantity and quality of data storage space that affects the users of cloud computing. With the increase of security and overall system strength, the customer base grows equally. Trust is one of the most important issues within cloud computing; increasing security and decreasing risks is the best way of achieving that trust.

Another important concern with cloud computing security is the sensitivity of the information that will be put into the cloud. The data can range from very general information to extremely confidential and important information. Some types of information can be classified as being too sensitive to be put into the cloud.

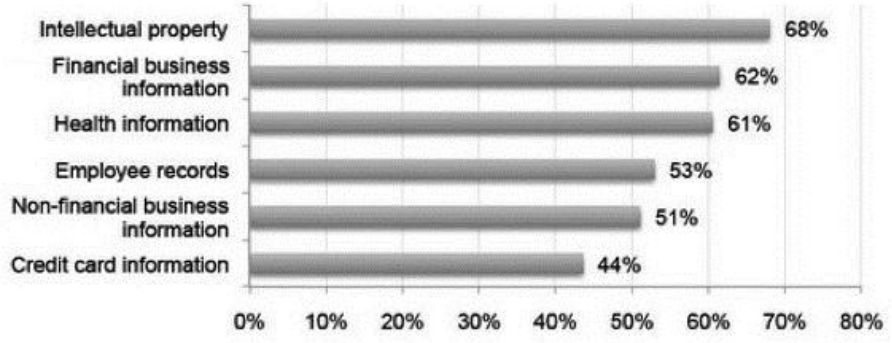

Figure 5: Types of Information Too Sensitive To Put in the Cloud (Vizard, 2010).

The above figure, again from the Ponemon Institute study, shows the percentages of information that is deemed too sensitive to put into the cloud. Intellectual property stands out on top at a staggering 68%. Although one might think the complete opposite, credit card information sits low at 44%. Cloud computing security standards have grown significantly over the past decade, and specific information that can be encrypted securely is at much less risk of being compromised than it once was. Hopefully, with the growth of security standards, all of the subjected types of information can be protected and secured without as much concern as there is now. This will depend greatly on factors such as design, implementation and growth within an organization as well as overall growth of cloud computing security in general.

RECOMMENDATIONS AND CONCLUSION

With these extensive legal complications and numerous security issues, CIOs are looking for a way to mitigate their risk while still utilizing cloud alternatives to reduce cost and lower time to market. While there may not be a one-size-fits-all solution on how to implement cloud

computing in your environment, the ideal solution begins with making sure that you are considering it as a viable alternative for your enterprise computing needs. In order to do this you must have a clear framework in place, which identifies where and when to utilize cloud computing and will aid in decision-making. Mark Tonsetic, program manager at Corporate Executive Board's Infrastructure Executive Council, says it's not an all-or-nothing proposition. Instead, he advises CIOs to "look at the cloud on an application-by-application, project-by-project basis" (Betts, 2009). Tonsetic recommends developing a decision framework using a scorecard, which will help guide CIOs as to when Cloud solutions are the best tool to use. His scorecard takes into account metrics such as strategy, capacity, security, disaster recovery, performance, architecture and integration, as well as vendor support, compliance and health (Betts, 2009).

Utilizing a decision framework or scorecard model will help organizations to first understand and classify their assets, before they can determine if a cloud solution is viable for that asset. The Cloud Security Alliance (CSA), Security Guide V3.0 walks through the basic process. First, identify the asset you are considering for cloud deployment. It may be data, applications, functions or even processes. "With cloud computing our data and applications don't need to reside in the same location, and we can choose to shift only parts of functions to the cloud. For example we can host our application and data in our own data center, while still outsourcing a portion of its functionality to the cloud through a Platform as a Service" Cloud Security Alliance, 2011b, p. 8). Second, evaluate that asset by asking questions that will tell you the importance of the data or function to the organization. Third, based on the evaluation of the asset, map it to potential cloud deployment models such as public, private, community or hybrid. At this point you have a good understanding of whether or not you are going to entertain a cloud computing solution. If you are going to continue to use the cloud, your next step will be to evaluate the potential cloud service models and providers. "Forrester recommends businesses look for four characteristics when selecting a service: a homogenous IT environment, industry certifications to prove its security strength, advanced threat intelligence and management capabilities, and a highly qualified security staff" (Rapport, 2011). In assessing cloud providers, The Cloud Security Alliance (CSA), Security Guide V3.0 makes the following recommendation:

> Customers should view cloud services and security as supply chain security issues. This means examining and assessing the provider's supply chain . . . to the extent possible. This also means examining the provider's own their party management. Assessment of third party service providers should specifically target the provider's incident management, business continuity and disaster recovery policies, and processes and procedures; and should include review of co-location and back-up facilities (p. 32).

IT also needs to understand that with the implementation of cloud computing, their role will change. "The growing availability of cloud-based services offers impatient users a channel for IT software and applications services at what the users consider low cost and low risk. This situation is reflected in Gartner's prediction that by 2015, 25% of enterprise IT expenditures for most organizations will be managed outside the IT department's budget" (Hunter, 2011, p. 2). IT needs to become the broker of cloud computing implementations to ensure that the enterprise continues to have their technology needs met. "IT departments should explore how they can

position themselves as Cloud Service Brokers to the enterprise by establishing a purchase process that accommodates cloud adoption and encourages business units to come to the IT organization for advice and support" (Hunter, 2011, p. 5).

"The transition from direct provider of services to a mixed role as provider and broker begins with a definition of the services offered, as captured by the combination of a service portfolio and service catalog" (Hunter, 2011, p. 2). Understand that this new role will require new skills for the IT staff. They will now become relationship and contract managers, not just technical gurus. Gartner's *Five Cloud Computing Trends that Will Affect Your Cloud Strategy Through 2015,* outlines these in Table 2 below (Cearley & Smith, 2012, p. 2):

Impacts	Top Recommendations
Formal decision frameworks facilitate cloud investment optimization.	• Develop a model to identify the legal, compliance and corporate sensitivity regarding your data (e.g., data classification scheme). • For particular workload/data combinations, map the anticipated benefits against the associated risks for public cloud services. • For any given project, consider the timing of the anticipated impact, and focus attention on projects with a near-term impact on the business versus those with a longer-term indirect impact.
Hybrid cloud computing is an imperative.	• Establish security, management and governance models to coordinate the use of internal and external services. • Focus near-term efforts on application and data integration, linking fixed internal and external applications with a hybrid solution. • Approach sophisticated integrated solutions, cloudbursting and dynamic execution cautiously, because these are the least-mature and most problematic hybrid approaches.
Cloud brokerage will facilitate cloud consumption.	• Position IT as an internal cloud services broker providing advice, guidance and intermediary service for the consumption of cloud services. • Evaluate third-party cloud services brokers that can facilitate the consumption of cloud services. • Train IT staff in relationship management to better enable them to manage cloud provider relationships and contracts.

Table 2: Impacts and Top Recommendations for Cloud Computing Trends Affecting Strategy (Cearley & Smith, 2012, p. 2).

However, a framework or scorecard to evaluate when and what cloud computing resources are appropriate to use for your assets is an extremely time consuming practice that will need to be continually updated as technology changes. This leaves open the possibility of relying on an outdated evaluation method, which can lead to potential security vulnerabilities when moving to cloud offerings. Organizations need to understand their data. Poorly understood data models or weak data protection policies increase the security risks when utilizing cloud solutions. Many organizations today are immature when it comes to data classification, retention, and protection policies.

Additionally, IT organizations may not shift seamlessly to a new role of cloud services broker. The skill set needed for this role is not necessarily built into the same people who have been guiding the technical decisions in enterprises across the nation. "For the first time in history, IT organizations are facing major platform and demographic changes all at once. As the public cloud arrives in force during the next decade, the generation of IT professionals who build

corporate IT into what it is today will retire en masse" (Hunter, 2011, p. 2). The impact on organizations may force a move into the cloud when organizations are not ready for it.

Recommendations in summary:

- Review the Cloud on an application-by-application, project-by-project basis
- Utilize a decision framework and scorecard
- Do your homework, select cloud service providers carefully that include:
  - Homogenous IT environment with industry certifications
  - Advanced threat intelligence and highly qualified security staff
- View Cloud services as a supply chain
- Develop IT as a broker of cloud computing
- Understand legal ramifications and indemnification clauses

Overall, cloud computing security has undergone several drastic changes over the past decade and continues to improve. As technology continues to progress and expand, this adds both risk and stress to the security of cloud computing. Compromised data can become detrimental to an organization and must be a main concern. The security issues related to cloud computing must not only be addressed prior to and during implementation, but also within analysis of future trends. The need for innovation within the field of cloud computing is a must. Using security methods such as retinal scans, thumbprint scans and other biometrical measures can surely help to deter brute force techniques. Nonetheless, the complexity and sophistication of hacker tactics continues to increase as well. The more valuable information put into the cloud, the more attention it will draw from hackers. Organizations must develop systems that protect confidential information both internally and externally. Trust becomes a major concern and must be developed, as human intervention is inevitable, to control and maintain these systems. Trust is also a significant concern for customers, and therefore becomes an issue for the vendor. Cost and security are extremely important and necessary from both a buyer and seller perspective. Efficiency is a key component to success. The cloud must be affordable and competitive financially, and offer the best protection possible. As cloud technology grows, the prices will decrease, while showing an increase in security standards making it an attractive proposition.

REFERENCES

Aggarwal, S., & McCabe, L. (2011). *Seeing the big picture: How global midsize businesses can use cloud ERP to drive growth* [White paper]. Retrieved from http://www.smb-gr.com/wp-content/uploads/2012/pdfs/NetSuite_OneWorld_Final_1.pdf

Amoroso, E. (2011, September 1). *The cloud can actually make data safer*. Retrieved from http://www.scmagazine.com/the-cloud-can-actually-make-data-safer/printarticle/209743/

Balduzzi, M. (2012). *A journey into the privacy and security risks of a cloud computing service* [PowerPoint slides]. Retrieved from http://www.blackhat.com/docs/webcast/April_Webcast_Presentation.pdf

Betts, M. (2009). Cloud computing: How to decide "when to cloud." *Computerworld*. Retrieved from http://blogs.computerworld.com/cloud_computing_how_to_decide_when_to_cloud

BMC Software. (2011). *Three steps to effective cloud planning and design* [White paper]. Retrieved from http://documents.bmc.com/products/documents/26/73/202673/202673.pdf

Brandel, M. (2010). *Cloud security in the real world: 4 examples*. Retrieved from http://www.csoonline.com/article/print/596820

Carvalhoh, M. (2011, October). SECaaS: Security as a service. *ISSA Journal*. Retrieved from https://www.issa.org/Library/Journals/2011/October/Carvalho-Security%20as%20a%20Service.pdf

Cearley, D. W., & Smith, D. M. (2012). *Five cloud computing trends that will affect your cloud strategy through 2015.* Stamford, CT: Gartner. Retrieved from http://bit.ly/NPMN5x

Cloud Security Alliance. (2010). *Top threats to cloud computing v 1.0* [White paper]. Retrieved from http://bit.ly/e3opi5

Cloud Security Alliance. (2011a). *Defined categories of service 2011* [White paper]. Retrieved from https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf

Cloud Security Alliance. (2011b). *Security guidance for critical areas of focus in cloud computing V3.0* [White paper]. Retrieved from https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Cloud Security Alliance. (2012a). *Certificate of cloud security knowledge.* Retrieved from https://cloudsecurityalliance.org/education/certificate-of-cloud-security-knowledge/

Cloud Security Alliance. (2012b). *Cloud controls matrix (CCM).* Retrieved from http://bit.ly/NLVbYd

Comazzetto, A. (2012). *Botnets: The dark side of cloud computing* [White paper]. Retrieved from http://www.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/sophos-botnets.aspx

Eddy, N. (2011, November 8). *McAfee launches cloud security platform updates*. Retrieved from http://www.channelinsider.com/c/a/Security/McAfee-Launches-Cloud-Security-Platform-Updates-711328/

Gartner Research. (2010). *Gartner says worldwide cloud services market to surpass $68 billion in 2010*. Stamford, CT: Author. Retrieved from http://www.gartner.com/it/page.jsp?id=1389313

Gens, F. (2009). *New IDC IT cloud services survey: Top benefits and challenges*. Retrieved from http://blogs.idc.com/ie/?p=730

GeoTrust. (2011). *Choosing a cloud provider with confidence: SSL Provides a secure bridge to the cloud* [White paper]. Retrieved from http://www.geotrust.com/resources/whitepapers/choosing-cloud-provider.pdf

Grance, T., & Jansen, W., (2011). *Guidelines on security and privacy in public cloud computing*. Retrieved from http://1.usa.gov/OaOcV2

Hawes, L. (2012). *The new IT manager, part 1: Trends affective IT in business* [White paper]. Retrieved from http://news.citrixonline.com/wp-content/uploads/2012/03/Trends-Affecting-IT.pdf

Hunter, R. (2011). *How IT can work with (not against) the cloud.* Stamford, CT: Gartner. Retrieved from http://bit.ly/Syi5l9

Intel IT Center. (2011). *Cloud security insights for IT strategic planning*. Santa Clara, CA: Intel Corporation. Retrieved from http://intel.ly/Pa2EQM

Knorr, E., & Gruman, G. (2009). *What cloud computing really means*. Retrieved from http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031

Kopee, D. (2008). *John McCarthy* [PowerPoint slides]. Retrieved from http://bit.ly/Pa2Gs0

Koretz, D. (2012). *The smartest way to protect websites and web apps from attacks*. Sunnyvale, CA: Juniper Networks. Retrieved from http://www.blackhat.com/docs/webcast/April_Black_Hat_Webcast_Mykonos.pdf

Lemos, R. (2012a, January 30). Cloud means more secure remote access. *Dark Reading*. Retrieved from http://bit.ly/zTxEfP

Lemos, R. (2012b, February 27). Cloud's future security depends on mobile. *Dark Reading*. Retrieved from http://bit.ly/ytlV43

Linthicum, D. (2011). *The future of cloud computing*. Retrieved from http://bit.ly/PHDmFY

McAfee Labs. (2012). *2012 threats predictions*. Santa Clara, CA: Author. Retrieved from http://bit.ly/Pa335T

Mohamed, A. (2009). *A history of cloud computing*. Retrieved from http://bit.ly/t9bTJH

Olavsrud, T., & Muse, D. (2012). *How secure is the cloud? IT pros speak up*. Retrieved from http://www.cio.com/article/703064/How_Secure_Is_the_Cloud_IT_Pros_Speak_Up

OpenCrowd. (2012). C*loud taxonomy*. New York, NY: Author

Parann-Nissany, G. (2012). What's the future for cloud security. Retrieved from http://cloudcomputing.sys-con.com/node/2198726

Rapport, M. (2011, January 12). Forrester analyst: Don't fear the cloud, prepare for it. *Credit Union Times Magazine.* Retrieved from http://www.cutimes.com/2011/01/12/forrester-analyst-dont-fear-the-cloud-prepare-for-it

Ried, S., & Kisker, H. (with Matzke, P., Bartels, A., & Lisserman, M.). (2011). *Sizing the cloud: A BT Futures Report: Understanding and quantifying the future of cloud computing*. Cambridge, MA: Forrester. Retrieved from http://bit.ly/OdJ80w

Scott, W. (2010). Cloud security: Is it really an issue for SMBs? *Computer Fraud & Security, 2010*(10), 14-15. doi: 10.1016/S1361-3723(10)70133-0.

Smith, D. M., Natis, Y. V., Petri, G., Bittman, T. J., Knipp, E., Malinverno, P., & Feiman, J. (2011). *Predicts 2012: Cloud computing is becoming a reality.* Retrieved from: http://www.gartner.com/id=1870118

Sophos. (2012a). *Safeguard encryption for cloud storage: Protect your data when it's stored in the cloud*. Retrieved from http://www.sophos.com/medialibrary/PDFs/factsheets/sophossafeguardencryptionforcloudstoragedsna.pdf

Sophos. (2012b). *Security threat report 2012*. Retrieved from http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf

Thibodeau, P. (2011). *The race to cloud standards gets crowded*. Retrieved from http://bit.ly/oQ02Ir

Trappler, T. J. (2011). *Making sure your cloud provider can protect your data as promised: Certifications and inspections should be included in your contract*. Retrieved from http://bit.ly/RKV2po

Vijayan, J. (2011) *Feds launch cloud security standards program*. Retrieved from http://bit.ly/vUpWVc

Violino, B. (2010). *Five cloud security trends experts see for 2011*. Retrieved from http://www.csoonline.com/article/647128/five-cloud-security-trends-experts-see-for-2011

Vizard, M. (2010). *The state of cloud computing security*. Retrieved from http://bit.ly/SyjKqI

WebTrust. (2012). *Overview of trust services*. Retrieved from http://www.webtrust.org/overview-of-trust-services/item64420.aspx

Zhu, Y., Hu, H., Ahn, G. –J., & Yau, S. S. (2012). Efficient audit service outsourcing for data integrity in clouds. *Journal of Systems and Software, 85*(5), 1083-1095. doi: 10.1016/j.jss.2011.12.024.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*, 583-592. doi: 10.1016/j.future.2010.12.006