Chapter 6

Security in the Cloud

6.1 Chapter Overview

As discussed at the beginning of this book, cloud service providers are leveraging virtualization technologies combined with self-service capabilities for computing resources via the Internet. In these service provider environments, virtual machines from multiple organizations have to be co-located on the same physical server in order to maximize the efficiencies of virtualization. Cloud service providers must learn from the managed service provider (MSP) model and ensure that their customers' applications and data are secure if they hope to retain their customer base and competitiveness. Today, enterprises are looking toward cloud computing horizons to expand their on-premises infrastructure, but most cannot afford the risk of compromising the security of their applications and data. For example, IDC recently conducted a survey[1] (see Figure 6.1) of 244 IT executives/CIOs and their line-of-business (LOB) colleagues to gauge their opinions and understand their companies' use of IT cloud services. Security ranked first as the greatest challenge or issue of cloud computing.

This chapter identifies current security concerns about cloud computing environments and describes the methodology for ensuring application and data security and compliance integrity for those resources that are moving from on-premises to public cloud environments. More important, this discussion focuses on why and how these resources should be protected in the Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) environments and offers security "best practices" for service providers and enterprises that are in or are contemplating

1. http://cloudsecurity.org/2008/10/14/biggest-cloud-challenge-security, retrieved 21 Feb 2009.

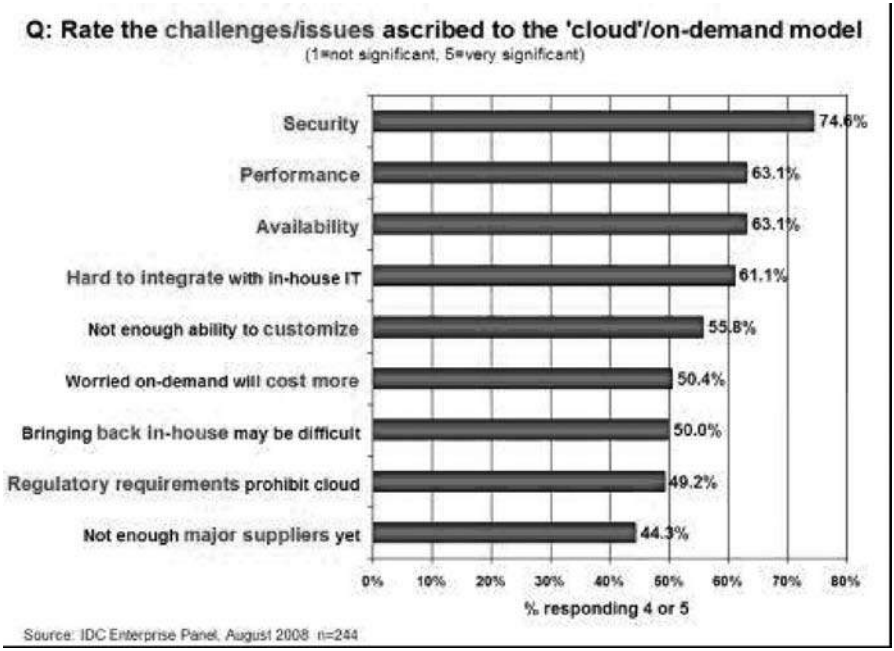

Figure 6.1 Results of IDC survey ranking security challenges.

moving into the cloud computing space. First, let's review the concepts of the three major cloud computing service provider models.

Software-as-a-Service is a model of software deployment in which an application is licensed for use as a service provided to customers on demand. On-demand licensing and use relieves the customer of the burden of equipping a device with every application to be used.[2] Gartner predicts that 30% of new software will be delivered via the SaaS model by 2010.

Platform-as-a-Service is an outgrowth of the SaaS application delivery model. With the PaaS model, all of the facilities required to support the complete life cycle of building and delivering web applications and services are available to developers, IT managers, and end users entirely from the Internet, without software downloads or installation. PaaS is also sometimes known as "cloudware." PaaS offerings include workflow facilities for application design, application development, testing, deployment, and hosting, as well as application services such as team collaboration, web service integration and marshalling, database integration, security, scalability, storage, persistence, state management, application versioning, application

2. http://en.wikipedia.org/wiki/Software_as_a_service.

instrumentation, and developer community facilitation. These services are provisioned as an integrated solution over the web.[3]

Infrastructure-as-a-Service is the delivery of computer infrastructure (typically a platform virtualization environment) as a service. These "virtual infrastructure stacks"[4] are an example of the everything-as-a-service trend and share many of the common characteristics. Rather than purchasing servers, software, data center space, or network equipment, clients buy these resources as a fully outsourced service. The service is typically billed on a utility computing basis, and the quantity of resources consumed (and therefore the cost) typically reflects the level of activity. It is an evolution of web hosting and virtual private server offerings.[5]

Inspired by the IT industry's move toward SaaS, in which software is not purchased but rented as a service from providers, **IT-as-a-Service (ITaaS)** is being proposed to take this concept further, to bring the service model right to your IT infrastructure. The modern IT organization must run itself as a separate operation and become more strategic in operational decisions. Many organizations are in the process of transforming their IT departments into self-sustaining cost-center operations, treating internal users as if they were customers.

This transformation is not trivial and usually involves elements of project portfolio management, workflow reengineering, and process improvement. The transformation can take several years to be completed. Many large IT organizations have adopted the Information Technology Infrastructure Library (ITIL) framework to help with this transformation. Organizations can harness their help desks, avoid downtime resulting from unauthorized changes, and deliver better service to their internal customers simply by adopting best practices for managing service requests, changes, and IT assets. The adoption of IT-as-a-Service can help enterprise IT functions focus on strategic alignment with business goals. However, if efforts in this direction are poorly implemented, organizations risk further alienating their technical support staff from the rest of the organization—turning them into order takers for the enterprise rather than business advisers. When it is done properly, a customer-centric IT

3. http://blogs.zdnet.com/Hinchcliffe/?p=166&tag=btxcsim; http://en.wikipedia.org/wiki/PaaS.
4. http://www.cbronline.com/article_feature.asp?guid=E66B8BF0-43BB-4AB1-9475-5884D82C897F.
5. http://en.wikipedia.org/wiki/IaaS.

department increases productivity, drives up project success rates, and creates a higher profile for technology within the organization.

While enterprises cope with defining the details of cloud computing, the single, unifying theme is *service*. Cloud computing, on-demand applications, and managed security are now perceived as part of an emerging ITaaS paradigm. Current industry buzz seems to reinforce the message that significant investments of capital, time, and intellectual resources are indeed being directed toward offering next-generation information and communication technology (ICT) infrastructure, which may allow enterprises to outsource IT completely and confidently. Only time will tell if ITaaS is really on the edge of enterprise adoption. Many in the industry believe that the advent of developer platforms designed for the cloud will hasten this transition and, as a result, fewer enterprises will need to deploy middleware to manage patchwork-implemented business applications, legacy or otherwise. Infrastructure vendors are also jumping on this bandwagon. Amazon has been a pioneer, with the release of Amazon S3 (Storage-as-a-Service). With the maturation of virtualization technologies, the adoption of virtual infrastructure and storage-on-demand services will accelerate along with the SaaS model.

There are some key financial benefits in moving to an ITaaS model, such has not having to incur capital costs; having a transparent, monthly pricing plan; scalability; and reasonable costs of expansion. Operational benefits of ITaaS include increased reliability because of a centralized infrastructure, which can ensure that critical services and applications are monitored continually; software flexibility, with centrally maintained products that allow for quick rollout of new functionalities and updates; and data security, since company data can be stored on owner-managed premises and backed up using encryption to a secure off-site data center.

Another service that is being discussed as we are writing this book is the concept of **Anything-as-a-Service (XaaS),** which is also a subset of cloud computing. XaaS broadly encompasses a process of activating reusable software components over the network. The most common and successful example is Software-as-a-Service. The growth of "as-a-service" offerings has been facilitated by extremely low barriers to entry (they are often accessible for free or available as recurring charges on a personal credit card). As a result, such offerings have been adopted by consumers and small businesses well before pushing into the enterprise space. All "as-a-service" offerings share a number of common attributes, including little or no capital expen-

diture since the required infrastructure is owned by the service provider, massive scalability, multitenancy, and device and location independence allowing consumers remote access to systems using nearly any current available technology.

On the surface, it appears that XaaS is a potentially game-changing technology that could reshape IT. However, most CIOs still depend on internal infrastructures because they are not convinced that cloud computing is ready for prime time. Many contend that if you want real reliability, you must write more reliable applications. Regardless of one's view on the readiness of cloud computing to meet corporate IT requirements, it cannot be ignored. The concept of pay-as-you-go applications, development platforms, processing power, storage, or any other cloud-enabled services has emerged and can be expected to reshape IT over the next decade.

Other concerns plague IT executives. They fear their data won't be safe in the hands of cloud providers and that they won't be able to manage cloud resources effectively. They may also worry that the new technology will threaten their own data centers and staff. Collectively, these fears tend to hold back the cloud computing market that some perceive growing to nearly $100 billion in the next decade.

Although there is a significant benefit to leveraging cloud computing, security concerns have led organizations to hesitate to move critical resources to the cloud. Corporations and individuals are often concerned about how security and compliance integrity can be maintained in this new environment. Even more worrying, however, may be those corporations that are jumping into cloud computing that may be oblivious to the implications of putting critical applications and data in the cloud. This chapter will answer the security concerns of the former and educate the latter.

Moving critical applications and sensitive data to public and shared cloud environments is of great concern for those corporations that are moving beyond their data center's network perimeter defense. To alleviate these concerns, a cloud solution provider must ensure that customers will continue to have the same security and privacy controls over their applications and services, provide evidence to customers that their organization and customers are secure and they can meet their service-level agreements, and that they can prove compliance to auditors.

6.2 Cloud Security Challenges

Although virtualization and cloud computing can help companies accomplish more by breaking the physical bonds between an IT infrastructure and its users, heightened security threats must be overcome in order to benefit fully from this new computing paradigm. This is particularly true for the SaaS provider. Some security concerns are worth more discussion. For example, in the cloud, you lose control over assets in some respects, so your security model must be reassessed. Enterprise security is only as good as the least reliable partner, department, or vendor. Can you trust your data to your service provider? In the following paragraphs, we discuss some issues you should consider before answering that question.

With the cloud model, you lose control over physical security. In a public cloud, you are sharing computing resources with other companies. In a shared pool outside the enterprise, you don't have any knowledge or control of where the resources run. Exposing your data in an environment shared with other companies could give the government "reasonable cause" to seize your assets because another company has violated the law. Simply because you share the environment in the cloud, may put your data at risk of seizure.

Storage services provided by one cloud vendor may be incompatible with another vendor's services should you decide to move from one to the other. Vendors are known for creating what the hosting world calls "sticky services"—services that an end user may have difficulty transporting from one cloud vendor to another (e.g., Amazon's "Simple Storage Service" [S3] is incompatible with IBM's Blue Cloud, or Google, or Dell).

If information is encrypted while passing through the cloud, who controls the encryption/decryption keys? Is it the customer or the cloud vendor? Most customers probably want their data encrypted both ways across the Internet using SSL (Secure Sockets Layer protocol). They also most likely want their data encrypted while it is at rest in the cloud vendor's storage pool. Be sure that you, the customer, control the encryption/decryption keys, just as if the data were still resident on your own servers.

Data integrity means ensuring that data is identically maintained during any operation (such as transfer, storage, or retrieval). Put simply, data integrity is assurance that the data is consistent and correct. Ensuring the integrity of the data really means that it changes only in response to

authorized transactions. This sounds good, but you must remember that a common standard to ensure data integrity does not yet exist.

Using SaaS offerings in the cloud means that there is much less need for software development. For example, using a web-based customer relationship management (CRM) offering eliminates the necessity to write code and "customize" a vendor's application. If you plan to use internally developed code in the cloud, it is even more important to have a formal secure software development life cycle (SDLC). The immature use of mashup technology (combinations of web services), which is fundamental to cloud applications, is inevitably going to cause unwitting security vulnerabilities in those applications. Your development tool of choice should have a security model embedded in it to guide developers during the development phase and restrict users only to their authorized data when the system is deployed into production.

As more and more mission-critical processes are moved to the cloud, SaaS suppliers will have to provide log data in a real-time, straightforward manner, probably for their administrators as well as their customers' personnel. Someone has to be responsible for monitoring for security and compliance, and unless the application and data are under the control of end users, they will not be able to. Will customers trust the cloud provider enough to push their mission-critical applications out to the cloud? Since the SaaS provider's logs are internal and not necessarily accessible externally or by clients or investigators, monitoring is difficult. Since access to logs is required for Payment Card Industry Data Security Standard (PCI DSS) compliance and may be requested by auditors and regulators, security managers need to make sure to negotiate access to the provider's logs as part of any service agreement.

Cloud applications undergo constant feature additions, and users must keep up to date with application improvements to be sure they are protected. The speed at which applications will change in the cloud will affect both the SDLC and security. For example, Microsoft's SDLC assumes that mission-critical software will have a three- to five-year period in which it will not change substantially, but the cloud may require a change in the application every few weeks. Even worse, a secure SLDC will not be able to provide a security cycle that keeps up with changes that occur so quickly. This means that users must constantly upgrade, because an older version may not function, or protect the data.

Having proper fail-over technology is a component of securing the cloud that is often overlooked. The company can survive if a non-mission-critical application goes offline, but this may not be true for mission-critical applications. Core business practices provide competitive differentiation. Security needs to move to the data level, so that enterprises can be sure their data is protected wherever it goes. Sensitive data is the domain of the enterprise, not the cloud computing provider. One of the key challenges in cloud computing is data-level security.

Most compliance standards do not envision compliance in a world of cloud computing. There is a huge body of standards that apply for IT security and compliance, governing most business interactions that will, over time, have to be translated to the cloud. SaaS makes the process of compliance more complicated, since it may be difficult for a customer to discern where its data resides on a network controlled by its SaaS provider, or a partner of that provider, which raises all sorts of compliance issues of data privacy, segregation, and security. Many compliance regulations require that data not be intermixed with other data, such as on shared servers or databases. Some countries have strict limits on what data about its citizens can be stored and for how long, and some banking regulators require that customers' financial data remain in their home country.

Compliance with government regulations such as the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA), and industry standards such as the PCI DSS, will be much more challenging in the SaaS environment. There is a perception that cloud computing removes data compliance responsibility; however, it should be emphasized that the data owner is still fully responsible for compliance. Those who adopt cloud computing must remember that it is the responsibility of the data owner, not the service provider, to secure valuable data.

Government policy will need to change in response to both the opportunity and the threats that cloud computing brings. This will likely focus on the off-shoring of personal data and protection of privacy, whether it is data being controlled by a third party or off-shored to another country. There will be a corresponding drop in security as the traditional controls such as VLANs (virtual local-area networks) and firewalls prove less effective during the transition to a virtualized environment. Security managers will need to pay particular attention to systems that contain critical data such as corporate

financial information or source code during the transition to server virtualization in production environments.

Outsourcing means losing significant control over data, and while this isn't a good idea from a security perspective, the business ease and financial savings will continue to increase the usage of these services. Security managers will need to work with their company's legal staff to ensure that appropriate contract terms are in place to protect corporate data and provide for acceptable service-level agreements.

Cloud-based services will result in many mobile IT users accessing business data and services without traversing the corporate network. This will increase the need for enterprises to place security controls between mobile users and cloud-based services. Placing large amounts of sensitive data in a globally accessible cloud leaves organizations open to large distributed threats—attackers no longer have to come onto the premises to steal data, and they can find it all in the one "virtual" location.

Virtualization efficiencies in the cloud require virtual machines from multiple organizations to be co-located on the same physical resources. Although traditional data center security still applies in the cloud environment, physical segregation and hardware-based security cannot protect against attacks between virtual machines on the same server. Administrative access is through the Internet rather than the controlled and restricted direct or on-premises connection that is adhered to in the traditional data center model. This increases risk and exposure and will require stringent monitoring for changes in system control and access control restriction.

The dynamic and fluid nature of virtual machines will make it difficult to maintain the consistency of security and ensure the auditability of records. The ease of cloning and distribution between physical servers could result in the propagation of configuration errors and other vulnerabilities. Proving the security state of a system and identifying the location of an insecure virtual machine will be challenging. Regardless of the location of the virtual machine within the virtual environment, the intrusion detection and prevention systems will need to be able to detect malicious activity at virtual machine level. The co-location of multiple virtual machines increases the attack surface and risk of virtual machine-to-virtual machine compromise.

Localized virtual machines and physical servers use the same operating systems as well as enterprise and web applications in a cloud server environment, increasing the threat of an attacker or malware exploiting vulnerabilities in these systems and applications remotely. Virtual machines are

vulnerable as they move between the private cloud and the public cloud. A fully or partially shared cloud environment is expected to have a greater attack surface and therefore can be considered to be at greater risk than a dedicated resources environment.

Operating system and application files are on a shared physical infrastructure in a virtualized cloud environment and require system, file, and activity monitoring to provide confidence and auditable proof to enterprise customers that their resources have not been compromised or tampered with. In the cloud computing environment, the enterprise subscribes to cloud computing resources, and the responsibility for patching is the subscriber's rather than the cloud computing vendor's. The need for patch maintenance vigilance is imperative. Lack of due diligence in this regard could rapidly make the task unmanageable or impossible, leaving you with "virtual patching" as the only alternative.

Enterprises are often required to prove that their security compliance is in accord with regulations, standards, and auditing practices, regardless of the location of the systems at which the data resides. Data is fluid in cloud computing and may reside in on-premises physical servers, on-premises virtual machines, or off-premises virtual machines running on cloud computing resources, and this will require some rethinking on the part of auditors and practitioners alike.

In the rush to take advantage of the benefits of cloud computing, not least of which is significant cost savings, many corporations are likely rushing into cloud computing without a serious consideration of the security implications. To establish zones of trust in the cloud, the virtual machines must be self-defending, effectively moving the perimeter to the virtual machine itself. Enterprise perimeter security (i.e., firewalls, demilitarized zones [DMZs], network segmentation, intrusion detection and prevention systems [IDS/IPS], monitoring tools, and the associated security policies) only controls the data that resides and transits behind the perimeter. In the cloud computing world, the cloud computing provider is in charge of customer data security and privacy.

6.3 Software-as-a-Service Security

Cloud computing models of the future will likely combine the use of SaaS (and other XaaS's as appropriate), utility computing, and Web 2.0 collaboration technologies to leverage the Internet to satisfy their customers' needs. New business models being developed as a result of the move to

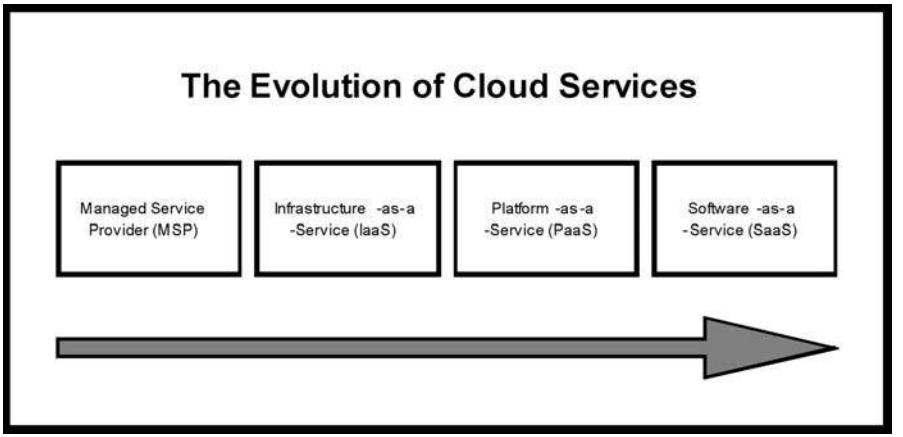

Figure 6.2 The evolution of cloud services.

cloud computing are creating not only new technologies and business operational processes but also new security requirements and challenges as described previously. As the most recent evolutionary step in the cloud service model (see Figure 6.2), SaaS will likely remain the dominant cloud service model for the foreseeable future and the area where the most critical need for security practices and oversight will reside.

Just as with an managed service provider, corporations or end users will need to research vendors' policies on data security before using vendor services to avoid losing or not being able to access their data. The technology analyst and consulting firm Gartner lists seven security issues which one should discuss with a cloud-computing vendor:

1. **Privileged user access**—Inquire about who has specialized access to data, and about the hiring and management of such administrators.
2. **Regulatory compliance**—Make sure that the vendor is willing to undergo external audits and/or security certifications.
3. **Data location**—Does the provider allow for any control over the location of data?
4. **Data segregation**—Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.

5. **Recovery**—Find out what will happen to data in the case of a disaster. Do they offer complete restoration? If so, how long would that take?
6. **Investigative support**—Does the vendor have the ability to investigate any inappropriate or illegal activity?
7. **Long-term viability**—What will happen to data if the company goes out of business? How will data be returned, and in what format?[6]

Determining data security is harder today, so data security functions have become more critical than they have been in the past. A tactic not covered by Gartner is to encrypt the data yourself. If you encrypt the data using a trusted algorithm, then regardless of the service provider's security and encryption policies, the data will only be accessible with the decryption keys. Of course, this leads to a follow-on problem: How do you manage private keys in a pay-on-demand computing infrastructure?[7]

To address the security issues listed above along with others mentioned earlier in the chapter, SaaS providers will need to incorporate and enhance security practices used by the managed service providers and develop new ones as the cloud computing environment evolves. The baseline security practices for the SaaS environment as currently formulated are discussed in the following sections.

6.3.1 Security Management (People)

One of the most important actions for a security team is to develop a formal charter for the security organization and program. This will foster a shared vision among the team of what security leadership is driving toward and expects, and will also foster "ownership" in the success of the collective team. The charter should be aligned with the strategic plan of the organization or company the security team works for. Lack of clearly defined roles and responsibilities, and agreement on expectations, can result in a general feeling of loss and confusion among the security team about what is expected of them, how their skills and experienced can be leveraged, and

6. http://www.infoworld.com/article/08/07/02/Gartner_Seven_cloudcomputing_security_risks_1.html, retrieved 20 Feb 2009.
7. http://en.wikipedia.org/wiki/Cloud_service#Cloud_storage, retrieved 15 Feb 2009.

meeting their performance goals. Morale among the team and pride in the team is lowered, and security suffers as a result.

6.3.2 Security Governance

A security steering committee should be developed whose objective is to focus on providing guidance about security initiatives and alignment with business and IT strategies. A charter for the security team is typically one of the first deliverables from the steering committee. This charter must clearly define the roles and responsibilities of the security team and other groups involved in performing information security functions. Lack of a formalized strategy can lead to an unsustainable operating model and security level as it evolves. In addition, lack of attention to security governance can result in key needs of the business not being met, including but not limited to, risk management, security monitoring, application security, and sales support. Lack of proper governance and management of duties can also result in potential security risks being left unaddressed and opportunities to improve the business being missed because the security team is not focused on the key security functions and activities that are critical to the business.

6.3.3 Risk Management

Effective risk management entails identification of technology assets; identification of data and its links to business processes, applications, and data stores; and assignment of ownership and custodial responsibilities. Actions should also include maintaining a repository of information assets. Owners have authority and accountability for information assets including protection requirements, and custodians implement confidentiality, integrity, availability, and privacy controls. A formal risk assessment process should be created that allocates security resources linked to business continuity.

6.3.4 Risk Assessment

Security risk assessment is critical to helping the information security organization make informed decisions when balancing the dueling priorities of business utility and protection of assets. Lack of attention to completing formalized risk assessments can contribute to an increase in information security audit findings, can jeopardize certification goals, and can lead to inefficient and ineffective selection of security controls that may not adequately mitigate information security risks to an acceptable level. A formal information security risk management process should proactively assess information security risks as well as plan and manage them on a periodic or

as-needed basis. More detailed and technical security risk assessments in the form of threat modeling should also be applied to applications and infrastructure. Doing so can help the product management and engineering groups to be more proactive in designing and testing the security of applications and systems and to collaborate more closely with the internal security team. Threat modeling requires both IT and business process knowledge, as well as technical knowledge of how the applications or systems under review work.

6.3.5 Security Portfolio Management

Given the fast pace and collaborative nature of cloud computing, security portfolio management is a fundamental component of ensuring efficient and effective operation of any information security program and organization. Lack of portfolio and project management discipline can lead to projects never being completed or never realizing their expected return; unsustainable and unrealistic workloads and expectations because projects are not prioritized according to strategy, goals, and resource capacity; and degradation of the system or processes due to the lack of supporting maintenance and sustaining organization planning. For every new project that a security team undertakes, the team should ensure that a project plan and project manager with appropriate training and experience is in place so that the project can be seen through to completion. Portfolio and project management capabilities can be enhanced by developing methodology, tools, and processes to support the expected complexity of projects that include both traditional business practices and cloud computing practices.

6.3.6 Security Awareness

People will remain the weakest link for security. Knowledge and culture are among the few effective tools to manage risks related to people. Not providing proper awareness and training to the people who may need them can expose the company to a variety of security risks for which people, rather than system or application vulnerabilities, are the threats and points of entry. Social engineering attacks, lower reporting of and slower responses to potential security incidents, and inadvertent customer data leaks are all possible and probable risks that may be triggered by lack of an effective security awareness program. The one-size-fits-all approach to security awareness is not necessarily the right approach for SaaS organizations; it is more important to have an information security awareness and training program that tailors the information and training according the individual's role in the

organization. For example, security awareness can be provided to development engineers in the form of secure code and testing training, while customer service representatives can be provided data privacy and security certification awareness training. Ideally, both a generic approach and an individual-role approach should be used.

6.3.7 Education and Training

Programs should be developed that provide a baseline for providing fundamental security and risk management skills and knowledge to the security team and their internal partners. This entails a formal process to assess and align skill sets to the needs of the security team and to provide adequate training and mentorship—providing a broad base of fundamental security, inclusive of data privacy, and risk management knowledge. As the cloud computing business model and its associated services change, the security challenges facing an organization will also change. Without adequate, current training and mentorship programs in place, the security team may not be prepared to address the needs of the business.

6.3.8 Policies, Standards, and Guidelines

Many resources and templates are available to aid in the development of information security policies, standards, and guidelines. A cloud computing security team should first identify the information security and business requirements unique to cloud computing, SaaS, and collaborative software application security. Policies should be developed, documented, and implemented, along with documentation for supporting standards and guidelines. To maintain relevancy, these policies, standards, and guidelines should be reviewed at regular intervals (at least annually) or when significant changes occur in the business or IT environment. Outdated policies, standards, and guidelines can result in inadvertent disclosure of information as a cloud computing organizational business model changes. It is important to maintain the accuracy and relevance of information security policies, standards, and guidelines as business initiatives, the business environment, and the risk landscape change. Such policies, standards, and guidelines also provide the building blocks with which an organization can ensure consistency of performance and maintain continuity of knowledge during times of resource turnover.

6.3.9 Secure Software Development Life Cycle (SecSDLC)

The SecSDLC involves identifying specific threats and the risks they represent, followed by design and implementation of specific controls to counter those threats and assist in managing the risks they pose to the organization and/or its customers. The SecSDLC must provide consistency, repeatability, and conformance. The SDLC consists of six phases, and there are steps unique to the SecSLDC in each of phases:

- **Phase 1.Investigation:** Define project processes and goals, and document them in the program security policy.
- **Phase 2.Analysis:** Analyze existing security policies and programs, analyze current threats and controls, examine legal issues, and perform risk analysis.
- **Phase 3.Logical design:** Develop a security blueprint, plan incident response actions, plan business responses to disaster, and determine the feasibility of continuing and/or outsourcing the project.
- **Phase 4.Physical design:** Select technologies to support the security blueprint, develop a definition of a successful solution, design physical security measures to support technological solutions, and review and approve plans.
- **Phase 5.Implementation:** Buy or develop security solutions. At the end of this phase, present a tested package to management for approval.
- **Phase 6.Maintenance:** Constantly monitor, test, modify, update, and repair to respond to changing threats.[8]

In the SecSDLC, application code is written in a consistent manner that can easily be audited and enhanced; core application services are provided in a common, structured, and repeatable manner; and framework modules are thoroughly tested for security issues before implementation and continuously retested for conformance through the software regression test cycle. Additional security processes are developed to support application development projects such as external and internal penetration testing and

8. Michael E. Whitman and Herbert J. Mattord, Management of Information Security, Thomson Course Technology, 2004, p. 57.

standard security requirements based on data classification. Formal training and communications should also be developed to raise awareness of process enhancements.

6.3.10 Security Monitoring and Incident Response

Centralized security information management systems should be used to provide notification of security vulnerabilities and to monitor systems continuously through automated technologies to identify potential issues. They should be integrated with network and other systems monitoring processes (e.g., security information management, security event management, security information and event management, and security operations centers that use these systems for dedicated 24/7/365 monitoring). Management of periodic, independent third-party security testing should also be included.

Many of the security threats and issues in SaaS center around application and data layers, so the types and sophistication of threats and attacks for a SaaS organization require a different approach to security monitoring than traditional infrastructure and perimeter monitoring. The organization may thus need to expand its security monitoring capabilities to include application- and data-level activities. This may also require subject-matter experts in applications security and the unique aspects of maintaining privacy in the cloud. Without this capability and expertise, a company may be unable to detect and prevent security threats and attacks to its customer data and service stability.

6.3.11 Third-Party Risk Management

As SaaS moves into cloud computing for the storage and processing of customer data, there is a higher expectation that the SaaS will effectively manage the security risks with third parties. Lack of a third-party risk management program may result in damage to the provider's reputation, revenue losses, and legal actions should the provider be found not to have performed due diligence on its third-party vendors.

6.3.12 Requests for Information and Sales Support

If you don't think that requests for information and sales support are part of a security team's responsibility, think again. They are part of the business, and particularly with SaaS, the integrity of the provider's security business model, regulatory and certification compliance, and your company's reputation, competitiveness, and marketability all depend on the security team's ability to provide honest, clear, and concise answers to a customer request

for information (RFI) or request for proposal (RFP). A structured process and a knowledge base of frequently requested information will result in considerable efficiency and the avoidance of ad-hoc, inefficient, or inconsistent support of the customer RFI/RFP process. Members of the security team should be not only internal security evangelists but also security evangelists to customers in support of the sales and marketing teams. As discussed earlier, security is top-of-mind and a primary concern for cloud computing customers, and lack of information security representatives who can provide support to the sales team in addressing customer questions and concerns could result in the potential loss of a sales opportunity.

6.3.13 Business Continuity Plan

The purpose of business continuity (BC)/disaster recovery (DR) planning is to minimize the impact of an adverse event on business processes. Business continuity and resiliency services help ensure uninterrupted operations across all layers of the business, as well as helping businesses avoid, prepare for, and recover from a disruption. SaaS services that enable uninterrupted communications not only can help the business recover from an outage, they can reduce the overall complexity, costs, and risks of day-to-day management of your most critical applications. The cloud also offers some dramatic opportunities for cost-effective BC/DR solutions.

Some of the advantages that SaaS can provide over traditional BC/DR are eliminating email downtime, ensuring that email messages are never lost, and making system outages virtually invisible to end users no matter what happens to your staff or infrastructure; maintaining continuous telephone communication during a telecommunication outage so your organization can stay open and in contact with employees, customers, and partners at virtually any location, over any network, over any talking device; and providing wireless continuity for WiFi-enabled "smart" phones that ensures users will always be able to send and receive corporate email from their WiFi-enabled devices, even if your corporate mail system, data center, network, and staff are unavailable.[9]

6.3.14 Forensics

Computer forensics is used to retrieve and analyze data. The practice of computer forensics means responding to an event by gathering and preserving data, analyzing data to reconstruct events, and assessing the state of an

9. http://www.eseminarslive.com/c/a/Cloud-Computing/Dell030509, retrieved 15 Feb 2009.

event. Network forensics includes recording and analyzing network events to determine the nature and source of information abuse, security attacks, and other such incidents on your network. This is typically achieved by recording or capturing packets long-term from a key point or points in your infrastructure (such as the core or firewall) and then data mining for analysis and re-creating content.[10]

Cloud computing can provide many advantages to both individual forensics investigators and their whole team. A dedicated forensic server can be built in the same cloud as the company cloud and can be placed offline but available for use when needed. This provides a cost-effective readiness factor because the company itself then does not face the logistical challenges involved. For example, a copy of a virtual machine can be given to multiple incident responders to distribute the forensic workload based on the job at hand or as new sources of evidence arise and need analysis. If a server in the cloud is compromised, it is possible to clone that server at the click of a mouse and make the cloned disks instantly available to the cloud forensics server, thus reducing evidence-acquisition time. In some cases, dealing with operations and trying to abstract the hardware from a data center may become a barrier to or at least slow down the process of doing forensics, especially if the system has to be taken down for a significant period of time while you search for the data and then hope you have the right physical acquisition toolkit and supports for the forensic software you are using.

Cloud computing provides the ability to avoid or eliminate disruption of operations and possible service downtime. Some cloud storage implementations expose a cryptographic checksum or hash (such as the Amazon S3 generation of an MD5 hash) when you store an object. This makes it possible to avoid the need to generate MD5 checksums using external tools—the checksums are already there, thus eliminating the need for forensic image verification time. In today's world, forensic examiners typically have to spend a lot of time consuming expensive provisioning of physical devices. Bit-by-bit copies are made more quickly by replicated, distributed file systems that cloud providers can engineer for their customers, so customers have to pay for storage only for as long as they need the. You can now test a wider range of candidate passwords in less time to speed investigations by accessing documents more quickly because of the significant increase in CPU power provided by cloud computing.[11]

10. http://www.bitcricket.com/downloads/Network%20Forensics.pdf, retrieved 15 Feb 2009.

6.3.15 Security Architecture Design

A security architecture framework should be established with consideration of processes (enterprise authentication and authorization, access control, confidentiality, integrity, nonrepudiation, security management, etc.), operational procedures, technology specifications, people and organizational management, and security program compliance and reporting. A security architecture document should be developed that defines security and privacy principles to meet business objectives. Documentation is required for management controls and metrics specific to asset classification and control, physical security, system access controls, network and computer management, application development and maintenance, business continuity, and compliance. A design and implementation program should also be integrated with the formal system development life cycle to include a business case, requirements definition, design, and implementation plans. Technology and design methods should be included, as well as the security processes necessary to provide the following services across all technology layers:

1. Authentication
2. Authorization
3. Availability
4. Confidentiality
5. Integrity
6. Accountability
7. Privacy

The creation of a secure architecture provides the engineers, data center operations personnel, and network operations personnel a common blueprint to design, build, and test the security of the applications and systems. Design reviews of new changes can be better assessed against this architecture to assure that they conform to the principles described in the architecture, allowing for more consistent and effective design reviews.

11. http://cloudsecurity.org/2008/07/21/assessing-the-security-benefits-of-cloud-computing, retrieved 15 Feb 2009.

6.3.16 Vulnerability Assessment

Vulnerability assessment classifies network assets to more efficiently prioritize vulnerability-mitigation programs, such as patching and system upgrading. It measures the effectiveness of risk mitigation by setting goals of reduced vulnerability exposure and faster mitigation. Vulnerability management should be integrated with discovery, patch management, and upgrade management processes to close vulnerabilities before they can be exploited.

6.3.17 Password Assurance Testing

If the SaaS security team or its customers want to periodically test password strength by running password "crackers," they can use cloud computing to decrease crack time and pay only for what they use. Instead of using a distributed password cracker to spread the load across nonproduction machines, you can now put those agents in dedicated compute instances to alleviate mixing sensitive credentials with other workloads.[12]

6.3.18 Logging for Compliance and Security Investigations

When your logs are in the cloud, you can leverage cloud computing to index those logs in real-time and get the benefit of instant search results. A true real-time view can be achieved, since the compute instances can be examined and scaled as needed based on the logging load. Due to concerns about performance degradation and log size, the use of extended logging through an operating system C2 audit trail is rarely enabled. If you are willing to pay for enhanced logging, cloud computing provides the option.

6.3.19 Security Images

With cloud computing, you don't have to do physical operating system installs that frequently require additional third-party tools, are time-consuming to clone, and can add another agent to each endpoint. Virtualization-based cloud computing provides the ability to create "Gold image" VM secure builds and to clone multiple copies.[13] Gold image VMs also provide the ability to keep security up to date and reduce exposure by patching offline. Offline VMs can be patched off-network, providing an easier, more cost-effective, and less production-threatening way to test the impact of security changes. This is a great way to duplicate a copy of your production environment, implement a security change, and test the impact at low cost,

12. http://cloudsecurity.org/2008/07/21/assessing-the-security-benefits-of-cloud-computing, retrieved 15 Feb 2009.

with minimal start-up time, and it removes a major barrier to doing security in a production environment.[14]

6.3.20 Data Privacy

A risk assessment and gap analysis of controls and procedures must be conducted. Based on this data, formal privacy processes and initiatives must be defined, managed, and sustained. As with security, privacy controls and protection must an element of the secure architecture design. Depending on the size of the organization and the scale of operations, either an individual or a team should be assigned and given responsibility for maintaining privacy.

A member of the security team who is responsible for privacy or a corporate security compliance team should collaborate with the company legal team to address data privacy issues and concerns. As with security, a privacy steering committee should also be created to help make decisions related to data privacy. Typically, the security compliance team, if one even exists, will not have formalized training on data privacy, which will limit the ability of the organization to address adequately the data privacy issues they currently face and will be continually challenged on in the future. The answer is to hire a consultant in this area, hire a privacy expert, or have one of your existing team members trained properly. This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators.

13. When companies create a pool of virtualized servers for production use, they also change their deployment and operational practices. Given the ability to standardize server images (since there are no hardware dependencies), companies consolidate their server configurations into as few as possible "gold images" which are used as templates for creating common server configurations. Typical images include baseline operating system images, web server images, application server images, etc. This standardization introduces an additional risk factor: monoculture. All the standardized images will share the same weaknesses. Whereas in a traditional data center there are firewalls and intrusion-prevention devices between servers, in a virtual environment there are no physical firewalls separating the virtual machines. What used to be a multitier architecture with firewalls separating the tiers becomes a pool of servers. A single exposed server can lead to a rapidly propagating threat that can jump from server to server. Standardization of images is like dry tinder to a fire: A single piece of malware can become a firestorm that engulfs the entire pool of servers. The potential for loss and vulnerability increases with the size of the pool—in proportion to the number of virtual guests, each of which brings its own vulnerabilities, creating a higher risk than in a single-instance virtual server. Moreover, the risk of the sum is greater than the sum of the risk of the parts, because the vulnerability of each system is itself subject to a "network effect." Each additional server in the pool multiplies the vulnerability of other servers in the pool. See http;//www.nemertes.com/issue_papers/virtulatization_risk_analysis.
14. http://cloudsecurity.org/2008/07/21/assessing-the-security-benefits-of-cloud-computing, retrieved 15 Feb 2009.

For example, customer contractual requirements/agreements for data privacy must be adhered to, accurate inventories of customer data, where it is stored, who can access it, and how it is used must be known, and, though often overlooked, RFI/RFP questions regarding privacy must answered accurately. This requires special skills, training, and experience that do not typically exist within a security team.

As companies move away from a service model under which they do not store customer data to one under which they do store customer data, the data privacy concerns of customers increase exponentially. This new service model pushes companies into the cloud computing space, where many companies do not have sufficient experience in dealing with customer privacy concerns, permanence of customer data throughout its globally distributed systems, cross-border data sharing, and compliance with regulatory or lawful intercept requirements.

6.3.21 Data Governance

A formal data governance framework that defines a system of decision rights and accountability for information-related processes should be developed. This framework should describe who can take what actions with what information, and when, under what circumstances, and using what methods. The data governance framework should include:

- Data inventory
- Data classification
- Data analysis (business intelligence)
- Data protection
- Data privacy
- Data retention/recovery/discovery
- Data destruction

6.3.22 Data Security

The ultimate challenge in cloud computing is data-level security, and sensitive data is the domain of the enterprise, not the cloud computing provider. Security will need to move to the data level so that enterprises can be sure their data is protected wherever it goes. For example, with data-level security, the enterprise can specify that this data is not allowed to go outside of the United States. It can also force encryption of certain types of

data, and permit only specified users to access the data. It can provide compliance with the Payment Card Industry Data Security Standard (PCI DSS). True unified end-to-end security in the cloud will likely requires an ecosystem of partners.

6.3.23 Application Security

Application security is one of the critical success factors for a world-class SaaS company. This is where the security features and requirements are defined and application security test results are reviewed. Application security processes, secure coding guidelines, training, and testing scripts and tools are typically a collaborative effort between the security and the development teams. Although product engineering will likely focus on the application layer, the security design of the application itself, and the infrastructure layers interacting with the application, the security team should provide the security requirements for the product development engineers to implement. This should be a collaborative effort between the security and product development team. External penetration testers are used for application source code reviews, and attack and penetration tests provide an objective review of the security of the application as well as assurance to customers that attack and penetration tests are performed regularly. Fragmented and undefined collaboration on application security can result in lower-quality design, coding efforts, and testing results.

Since many connections between companies and their SaaS providers are through the web, providers should secure their web applications by following Open Web Application Security Project (OWASP)[15] guidelines for secure application development (mirroring Requirement 6.5 of the PCI DSS, which mandates compliance with OWASP coding practices) and locking down ports and unnecessary commands on Linux, Apache, MySQL, and PHP (LAMP) stacks in the cloud, just as you would on-premises. LAMP is an open-source web development platform, also called a web stack, that uses Linux as the operating system, Apache as the web server, MySQL as the relational database management system RDBMS, and PHP as the object-oriented scripting language. Perl or Python is often substituted for PHP.[16]

15. http://www.owasp.org/index.php/Main_Page, retrieved 15 Feb 2009.
16. http://www.webopedia.com/TERM/L/LAMP.html, retrieved 15 Feb 2009.

6.3.24 Virtual Machine Security

In the cloud environment, physical servers are consolidated to multiple virtual machine instances on virtualized servers. Not only can data center security teams replicate typical security controls for the data center at large to secure the virtual machines, they can also advise their customers on how to prepare these machines for migration to a cloud environment when appropriate.

Firewalls, intrusion detection and prevention, integrity monitoring, and log inspection can all be deployed as software on virtual machines to increase protection and maintain compliance integrity of servers and applications as virtual resources move from on-premises to public cloud environments. By deploying this traditional line of defense to the virtual machine itself, you can enable critical applications and data to be moved to the cloud securely. To facilitate the centralized management of a server firewall policy, the security software loaded onto a virtual machine should include a bidirectional stateful firewall that enables virtual machine isolation and location awareness, thereby enabling a tightened policy and the flexibility to move the virtual machine from on-premises to cloud resources. Integrity monitoring and log inspection software must be applied at the virtual machine level.

This approach to virtual machine security, which connects the machine back to the mother ship, has some advantages in that the security software can be put into a single software agent that provides for consistent control and management throughout the cloud while integrating seamlessly back into existing security infrastructure investments, providing economies of scale, deployment, and cost savings for both the service provider and the enterprise.

6.3.25 Identity Access Management (IAM)

As discussed in Chapter 5, identity and access management is a critical function for every organization, and a fundamental expectation of SaaS customers is that the principle of least privilege is granted to their data. The principle of least privilege states that only the minimum access necessary to perform an operation should be granted, and that access should be granted only for the minimum amount of time necessary.[17] However, business and IT groups will need and expect access to systems and applica-

17. http://web.mit.edu/Saltzer/www/publications/protection/Basic.html, retrieved 15 Feb 2009.

tions. The advent of cloud services and services on demand is changing the identity management landscape. Most of the current identity management solutions are focused on the enterprise and typically are architected to work in a very controlled, static environment. User-centric identity management solutions such as federated identity management, as mentioned in Chapter 5, also make some assumptions about the parties involved and their related services.

In the cloud environment, where services are offered on demand and they can continuously evolve, aspects of current models such as trust assumptions, privacy implications, and operational aspects of authentication and authorization, will be challenged. Meeting these challenges will require a balancing act for SaaS providers as they evaluate new models and management processes for IAM to provide end-to-end trust and identity throughout the cloud and the enterprise. Another issue will be finding the right balance between usability and security. If a good balance is not achieved, both business and IT groups may be affected by barriers to completing their support and maintenance activities efficiently.

6.3.26 Change Management

Although it is not directly a security issue, approving production change requests that do not meet security requirements or that introduce a security vulnerability to the production environment may result in service disruptions or loss of customer data. A successful security team typically collaborates with the operations team to review production changes as they are being developed and tested. The security team may also create security guidelines for standards and minor changes, to provide self-service capabilities for these changes and to prioritize the security team's time and resources on more complex and important changes to production.

6.3.27 Physical Security

Customers essentially lose control over physical security when they move to the cloud, since the actual servers can be anywhere the provider decides to put them. Since you lose some control over your assets, your security model may need to be reevaluated. The concept of the cloud can be misleading at times, and people forget that everything is somewhere actually tied to a physical location. The massive investment required to build the level of security required for physical data centers is the prime reason that companies don't build their own data centers, and one of several reasons why they are moving to cloud services in the first place.

For the SaaS provider, physical security is very important, since it is the first layer in any security model. Data centers must deliver multilevel physical security because mission-critical Internet operations require the highest level of security. The elements of physical security are also a key element in ensuring that data center operations and delivery teams can provide continuous and authenticated uptime of greater than 99.9999%. The key components of data center physical security are the following:

- Physical access control and monitoring, including 24/7/365 on-site security, biometric hand geometry readers inside "man traps," bullet-resistant walls, concrete bollards, closed-circuit TV (CCTV) integrated video, and silent alarms. Security personnel should request government-issued identification from visitors, and should record each visit. Security cameras should monitor activity throughout the facility, including equipment areas, corridors, and mechanical, shipping, and receiving areas. Motion detectors and alarms should be located throughout the facilities, and silent alarms should automatically notify security and law enforcement personnel in the event of a security breach.
- Environmental controls and backup power: Heat, temperature, air flow, and humidity should all be kept within optimum ranges for the computer equipment housed on-site. Everything should be protected by fire-suppression systems, activated by a dual-alarm matrix of smoke, fire, and heat sensors located throughout the entire facility. Redundant power links to two different local utilities should also be created where possible and fed through additional batteries and UPS power sources to regulate the flow and prevent spikes, surges, and brownouts. Multiple diesel generators should be in place and ready to provide clean transfer of power in the event that both utilities fail.
- Policies, processes, and procedures: As with information security, policies, processes, and procedures are critical elements of successful physical security that can protect the equipment and data housed in the hosting center.

6.3.28 Business Continuity and Disaster Recovery

In the SaaS environment, customers rely heavily on 24/7 access to their services, and any interruption in access can be catastrophic. The availability of

your software applications is the definition of your company's service and the life blood of your organization. Given the virtualization of the SaaS environment, the same technology will increasingly be used to support business continuity and disaster recovery, because virtualization software effectively "decouples" application stacks from the underlying hardware, and a virtual server can be copied, backed up, and moved just like a file. A growing number of virtualization software vendors have incorporated the ability to support live migrations. This, plus the decoupling capability, provides a low-cost means of quickly reallocating computing resources without any downtime. Another benefit of virtualization in business continuity and disaster recovery is its ability to deliver on service-level agreements and provide high-quality service.

Code escrow is another possibility, but object code is equivalent to source code when it comes to a SaaS provider, and the transfer and storage of that data must be tightly controlled. For the same reason that developer will not automatically provide source code outside their control when they license their software, it will be a challenge for SaaS escrow account providers to obtain a copy of the object code from a SaaS provider. Of course, the data center and its associated physical infrastructure will fall under standard business continuity and disaster recovery practices.

6.3.29 The Business Continuity Plan

A business continuity plan should include planning for non-IT-related aspects such as key personnel, facilities, crisis communication, and reputation protection, and it should refer to the disaster recovery plan for IT-related infrastructure recovery/continuity. The BC plan manual typically has five main phases: analysis, solution design, implementation, testing, and organization acceptance and maintenance. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure. Disaster recovery is the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.[18,19]

18. http://en.wikipedia.org/wiki/Business_continuity_planning, retrieved 21 Feb 2009.
19. http://en.wikipedia.org/wiki/Disaster_recovery, retrieved 21 Feb 2009.

6.4 Is Security-as-a-Service the New MSSP?

Managed security service providers (MSSPs) were the key providers of security in the cloud that was created by Exodus Communications, Global Crossing, Digital Island, and others that dominated the outsourced hosting environments that were the norm for corporations from the mid-1990s to the early 2000's. The cloud is essentially the next evolution of that environment, and many of the security challenges and management requirements will be similar. An MSSP is essentially an Internet service provider (ISP) that provides an organization with some network security management and monitoring (e.g., security information management, security event management, and security information and event management, which may include virus blocking, spam blocking, intrusion detection, firewalls, and virtual private network [VPN] management and may also handle system changes, modifications, and upgrades. As a result of the .dot.com bust and the subsequent Chapter 11 bankruptcies of many of the dominant hosting service providers, some MSSPs pulled the plug on their customers with short or no notice. With the increasing reluctance of organizations to give up complete control over the security of their systems, the MSSP market has dwindled over the last few years. The evolution to cloud computing has changed all this, and managed service providers that have survived are reinventing themselves along with a new concept of MSSP, which is now called Security-as-a-Service (SaaS)—not to be confused with Software-as-a-Service (SaaS), although it can be a component of the latter as well as other cloud services such as PaaS, IaaS, and MaaS.

Unlike MSSP, Security-as-a-Service does not require customers to give up complete control over their security posture. Customer system or security administrators have control over their security policies, system upgrades, device status and history, current and past patch levels, and outstanding support issues, on demand, through a web-based interface. Certain aspects of security are uniquely designed to be optimized for delivery as a web-based service, including:

- Offerings that require constant updating to combat new threats, such as antivirus and anti-spyware software for consumers
- Offerings that require a high level of expertise, often not found in-house, and that can be conducted remotely. These include ongoing

maintenance, scanning, patch management, and troubleshooting of security devices.

- Offerings that manage time- and resource-intensive tasks, which may be cheaper to outsource and offshore, delivering results and findings via a web-based solution. These include tasks such as log management, asset management, and authentication management.[20]

6.5 Chapter Summary

Virtualization is being used in data centers to facilitate cost savings and create a smaller, "green" footprint. As a result, multitenant uses of servers are being created on what used to be single-tenant or single-purpose physical servers. The extension of virtualization and virtual machines into the cloud is affecting enterprise security as a result of the evaporating enterprise network perimeter—the de-perimeterization of the enterprise, if you will. In this chapter, we discussed the importance of security in the cloud computing environment, particularly with regard to the SaaS environment and the security challenges and best practices associated with it.

In the next chapter, we will discuss the standards associated with cloud computing. Regardless of how the cloud evolves, it needs some form of standardization so that the market can evolve and thrive. Standards also allow clouds to interoperate and communicate with each other.

20. "Security as a Service," http://en.wikipedia.org/wiki/Security_as_a_service, retrieved 20 Feb 2009.