Unit 4

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.

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. Simply because you share the environment in the cloud, may put your data at risk.

Storage services and its security 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.

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.

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.

Software-as-a-service (SaaS) security issues

Cloud computing models of the future will likely combine the use of SaaS (and other as a service 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 cloud computing are creating not only new technologies and business operational processes but also new security requirements and challenges as described previously. 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. 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?

To address the security issues listed above along with others mentioned earlier in the topic, 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

Security Management

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

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.

Risk/ Vulnerability 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.

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 threat and attacks to its customer data and service stability.

Incident response is an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. An incident response plan includes a policy that defines, in specific terms, what constitutes an incident and provides a step-by-step process that should be followed when an incident occurs. An organization's incident response is conducted by the computer incident response team, a carefully selected group that, in addition to security and general IT staff, may include representatives from legal, human resources, and public relations departments.

Security Architecture Design

Security Architecture is one component of a products/systems overall architecture and is developed to provide guidance during the design of the product/system.

A security architecture framework should be established with consideration of processes (enterprise authentication and authorization, access control, confidentiality, integrity, non-repudiation, 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.

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.

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.

A vulnerability assessment attempts to identify the exposed vulnerabilities of a specific host, or possibly an entire network. The vulnerabilities may be due to configuration problems or missing software patches.

Vulnerability Assessment in cloud should be done in periodic basis with predefined service level agreement. Customers should be allowed to test cloud infrastructure before and after they outsource their infrastructure to cloud.

Data Privacy and Security

Cloud computing has transformed the way organizations approach IT, enabling them to become more agile, introduce new business models, provide more services, and reduce IT costs. Cloud computing technologies can be implemented in a wide variety of architectures, under different service and deployment models, and can coexist with other technologies and software design approaches.

Maintaining control over the data is paramount to cloud success. A decade ago, enterprise data typically resided in the organization's physical infrastructure, on its own servers in the enterprise's data center, where one could segregate sensitive data in individual physical servers. Today, with virtualization and the cloud, data may be under the organization's logical control, but physically reside in infrastructure owned and managed by another entity.

This shift in control is the number one reason new approaches and techniques are required to ensure organizations can maintain data security. When an outside party owns, controls, and manages infrastructure and computational resources, how can you be assured that business or regulatory data remains private and secure, and that your organization is protected from damaging data breaches—and feel you can still completely satisfy the full range of reporting, compliance, and regulatory requirements?

Some of the points to keep data private and secure in cloud infrastructure are as below:

1. Avoid storing sensitive information in the cloud.
2. Read the user agreement to find out how your cloud service storage works.
3. Password sensitivity
4. Encrypt your data
5. Use Encrypted cloud services

Application Security

Application security is one of the critical success factors for 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 team.

Although product engineers 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.

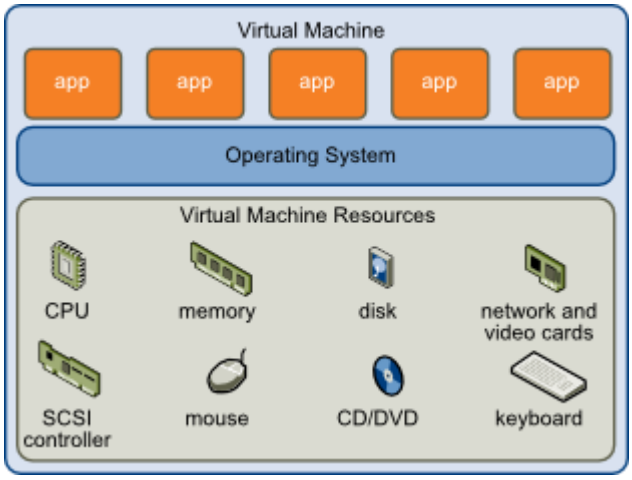
Some of the things that we should consider while moving to cloud application are:

a. Risks associated with cloud application
b. The fact that someone is managing and controlling your critical application
c. The perimeter of cloud is different and multitenant
d. Application should be protected with industry standard firewall and security products
e. Insecure Interfaces and Application Program Interface (API's)
f. Denial of Service (DOS) attack

Virtual Machine Security

Virtual machines are the containers in which applications and guest operating systems run. By design, all VMware virtual machines are isolated from one another. This isolation enables multiple virtual machines to run securely while sharing hardware and ensures both their ability to access hardware and their uninterrupted performance.

Each virtual machine is isolated from other virtual machines running on the same hardware. Although virtual machines share physical resources such as CPU, memory, and I/O devices, a guest operating system on an individual virtual machine cannot detect any device other than the virtual devices made available to it,



Virtual Machine Isolation

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.

A further area of concern with virtualization has to do with the potential for undetected network attacks between VMs collocated on a physical server. Unless you can monitor the traffic from each VM, you can't verify that traffic isn't possible between those VMs.
In essence, network virtualization must deliver an appropriate network interface to the VM. That interface might be a multiplexed channel with all the switching and routing handled in the network interconnect hardware.

Disaster Recovery

A Disaster Recovery Plan (DRP) is a business plan that describes how work can be resumed quickly and effectively after a disaster. Disaster recovery planning is just part of business continuity planning and applied to aspects of an organization that rely on an IT infrastructure to function.

The overall idea is to develop a plan that will allow the IT department to recover enough data and system functionality to allow a business or organization to operate - even possibly at a minimal level.

A **disaster recovery plan (DRP)** documents policies, procedures and actions to limit the disruption to an organization in the wake of a disaster. Just as a disaster is an event that makes the continuation of normal functions impossible, a disaster recovery plan consists of actions intended to minimize the negative effects of a disaster and allow the organization to maintain or quickly resume mission-critical functions.

To better understand and evaluate disaster recovery strategies, it is important to define two terms: recovery time objective (RTO) and recovery point objective (RPO).

RTO

The recovery time objective (RTO) is the maximum amount of time allocated for restoring application functionality. This is based on business requirements and is related to the importance of the application. Critical business applications require a low RTO.

RPO

The recovery point objective (RPO) is the acceptable time window of lost data due to the recovery process. For example, if the RPO is one hour, you must completely back up or replicate the data at least every hour. Once you bring up the application in an alternate datacenter, the backup data may be missing up to an hour of data. Like RTO, critical applications target a much smaller RPO.

Some of the points why Disaster Recovery is needed?

a. Machines, hardware and even data centers fail.
b. Much like machines, humans are not perfect. They make mistakes. In case of mistakes, DR may help resume business from back date.
c. Customers expect perfection as they don't want disruption in services
d. DR enabled organizations will attract more customers.

Disaster Recovery Management/ Planning Steps

- **Count the costs.** Although data center downtime is harmful to any company that relies on its IT services, it costs some companies more than others. Your disaster recovery plan should enable a fast return to service, but it shouldn't cost you more than you are losing in downtime costs.

- **Evaluate the types of threats you face and how extensively they can affect your facility.** Malicious attacks can occur anywhere, but you may also face threats peculiar to your location, such as weather events (tornadoes, hurricanes, floods and so on), earthquakes or other dangers. Part of preparing for a disaster is to know what is likely to occur and how those threats could affect your systems. Evaluating these situations beforehand allows you to better take appropriate action should one of these events occur.

- **Know what you have and how critical it is to operations.** Responding to a disaster in your data center is similar to doing so in medicine: you need to treat the more serious problems first, then the more minor ones. By determining which systems are most critical to your data center, you enable your IT staff to prioritize and make the best use of the precious minutes and hours immediately following an outage. Not every system need be functional immediately following a disaster.

- **Identify critical personnel and gather their contact information.** Who do you most want to be present in the data center following an outage? Who has the most expertise in a given area and the greatest ability to oversee some part of the recovery effort? Being able to get in touch with these people is crucial to a fast recovery. Collect their contact information and, just as importantly, keep it up to date. If it's been a year or more since you last checked, some of that contact information is likely out of date. Every minute you spend trying to find important personnel is time not spent on recovery.

- **Train your employees.** Knowledge of how to implement disaster recovery procedures is obviously important when an outage occurs. To this end, prepare by training personnel—

and not just in their respective areas of expertise. Everyone should have some broad-based knowledge of the recovery process so that it can be at least started even if not everyone is present.

- **Ensure that everyone knows the disaster recovery plan and understands his or her role.** Announcing the plan and assigning roles is not something you should do after a disaster strikes; it should be done well in advance, leaving time for personnel to learn their roles and to practice them. Almost nothing about a disaster event should be new (aside from some contingencies of the moment, perhaps): the IT staff should implement disaster recovery as a periodic task (almost) like any other.

- **Practice.** Needless to say, this is perhaps the most critical part of preparation for a downtime event. The difference between knowing your role and being able to execute it well is simply practice. You may not be able to shut down your data center to simulate precisely all of the conditions you will face in an outage, but you can go through many of the procedures nevertheless. Some recommendations prescribe semiannual drills, at a minimum, to practice implementing the disaster recovery plan. If there's one thing you take from this article, it's that you should practice your disaster recovery plan—don't expect it to unfold smoothly when you need it (regardless of how well laid-out a plan it is) if you haven't given it a trial run or two.

- **Automate where possible.** Your staff is limited, so it can only do so much. The more that your systems can do on their own in a recovery situation, the faster the recovery will generally be. This also leaves less room for human error—particularly in the kind of stressful atmosphere that exists following a disaster.

- **Follow up after a disaster.** When a downtime event does occur, evaluate the performance of the personnel and the plan to determine if any improvements can be made. Update your plan accordingly to enable a better response in the future. Furthermore, investigate the cause of the outage. If it's an internal problem, take necessary measures to correct equipment issues to avoid the same problem occurring again.