Unit-4

5. Federation, Presence, Identity, and Privacy in the Cloud

5.1 Chapter Overview

5.2 Federation in the Cloud

-Microsoft's Geneva has been described as a claims-based access platform and is said to help simplify access to applications and other systems. The concept allows for multiple providers to interact seamlessly with others, and it enables developers to incorporate various authentication models that will work with any corporate identity system. Here we deal with providing federation in the cloud through use of the Internet Engineering Task Force (IETF) standard, Extensible Messaging and Presence Protocol (XMPP) and inter domain federation using the Jabber Extensible Communications Platform (Jabber XCP), because this protocol is currently used by a wide range of existing services offered by providers as diverse as Google Talk, Live Journal, Earthlink, Facebook, ooVoo, Meebo, Twitter, the U.S. Marines Corps, the Defense Information Systems Agency

(DISA), the U.S. Joint Forces Command (USJFCOM), and the National Weather Service.

-XMPP's advantages include:

- It is decentralized, meaning anyone may set up an XMPP server.
- It is based on open standards.
- It is mature—multiple implementations of clients and servers exist.
- Robust security is supported via Simple Authentication and Security Layer (SASL) and Transport Layer Security (TLS).
- It is flexible and designed to be extended.

5.2.1 Four Levels of Federation

-Federation is the ability for two XMPP servers in different domains to exchange XML stanzas.

1. Permissive federation: Permissive federation occurs when a server accepts a connection from a peer network server without verifying its identity using DNS look-ups or certificate checking.
2. Verified federation: This type of federation occurs when a server accepts a connection from a peer after the identity of the peer has been verified.
3. Encrypted federation: In this mode, a server accepts a connection from a peer if and only if the peer supports Transport Layer Security (TLS) as defined for XMPP
4. Trusted federation: Here, a server accepts a connection from a peer only under the stipulation that the peer supports TLS and the peer can present a digital certificate issued by a root certification authority (CA)

5.2.2 How Encrypted Federation Differs from Trusted Federation

-Verified federation serves as a foundation for encrypted federation, which builds on it concepts by requiring use of TLS for channel encryption. Trusted federations provides strong authentication.

5.2.3 Federated Services and Applications

-Clouds typically consist of all the users, devices, services, and applications connected to the network. Finding these entities is a process called discovery. XMPP uses service discovery (as defined in XEP-0030) to find the aforementioned entities.

5.2.4 Protecting and Controlling Federated Communication

-The need for protecting federated communications Measures:
Designers of technologies like XMPP learned from past problems with email systems and incorporated these lessons to prevent address spoofing, unlimited binary attachments, inline scripts, and other attack tactics in XMPP.

The use of point-to-point federation will avoid problem that occur with multi-hop federation. This includes injection attacks, data loss, and unencrypted intermediate links. Using certificates issued by trusted root CAs ensures encrypted connections and strong authentication, both of which are currently feasible with an email network. Employing intelligent servers that have the ability to blacklist (explicitly block) and whitelist (explicitly permit) foreign services, either at the host level or the IP address level, is a significant mitigating factor.

5.2.5 The Future of Federation

-The process of server-to-server federation for the purpose of inter-domain communication has played a large role in the success of XMPP, which relies on a small set of simple but powerful mechanisms for domain checking and security to generate verified, encrypted, and trusted connections between any two deployed servers.

5.3 Presence in the Cloud

-provides true-or-false answers to queries about the network availability of a person, device, or application. Presence is a core component of an entity's real-time identity. Presence serves as a catalyst for communication. Its purpose is to signal availability for interaction over a network. It is being used to determine availability for phones, conference rooms, applications, web-based services, routers, firewalls, servers, appliances, buildings, devices, and other applications.

-Implementation of presence follows the software design pattern known as publish-and subscribe (pub-sub). This means that a user or application publishes information about its network availability to a centralized location and that information is broadcast to all entities that are authorized to receive it.

5.3.1 Presence Protocols

-Proprietary, consumer-oriented messaging services do not enable enterprises or institutions to leverage the power of presence. A smarter approach is to use one of the standard presence protocols, SIMPLE or XMPP. is an instant messaging and presence protocol suite based on SIP and managed by the Internet Engineering Task Force (IETF).

5.3.2 Leveraging Presence

-The real challenge today is to figure out how to leverage the power of presence within an organization or service offering. This requires having the ability to publish presence information from a wide range of data sources, the ability to receive or embed presence information in just about any platform or application, and having a robust presence engine to tie ubiquitous publishers and subscribers together.

5.3.3 Presence Enabled

-Providing presence data through as many avenues as possible is in large measure the responsibility of a presence engine.

-Being able to operate using multiple protocols such as IMPS, SIMPLE, and XMPP is a basic requirement in order to distribute presence information as widely as possible.

5.3.4 The Future of Presence

-It will remain to be seen if XMPP is the future of cloud services, but for now it is the dominant protocol for presence in the space.

5.3.5 The Interrelation of Identity, Presence and Location in the Cloud

-*Digital identity* refers to the traits, attributes, and preferences on which one may receive personalized services. Identity traits might include government issued IDs, corporate user accounts, and biometric information. Two user attributes which may be associated with identity are presence and location.
-Presence is most often associated with real-time communications systems such as IM and describes the state of a user's interaction with a system, such as which computer they are accessing, whether they are idle or working, and perhaps also which task they are currently performing (reading a document, composing email etc.).
-Location refers to the user's physical location and typically includes latitude, longitude, and (sometimes) altitude. Authentication and authorization mechanisms generally focus on determining the "who" of identity, location defines the "where," and presence defines the "what"—all critical components of the identity-based emerging technologies listed above, including cloud computing.

5.3.6 Federated Identity Management

-Federated identity management (IdM) refers to standards-based approaches for handling authentication, single sign-on (SSO, a property of access control for multiple related but independent software systems), role-based access control, and session management across diverse organizations, security domains, and application platforms. It is a system that allows individuals to use the same user name, password, or other personal identification to sign on to the networks of more than one entity in order to conduct transactions.

5.3.7 Cloud and SaaS Identity Management

-With the success of single sign-on inside the enterprise, users are calling for interoperability outside the enterprise's security domain to outsourced services, including business process outsourcing (BPO) and SaaS providers, and trading partners, as well as within the enterprise to affiliates and subsidiaries. As a result of business demands that employees be able to traverse the Internet with highly sensitive data, using secure connections that protect the user, the enterprise, and the service provider, Internet-based SSO has seen a substantial increase over the last few years.

5.3.8 Federating Identity

-The most successful way to achieve identity federation is to choose a standalone federation vendor, whose sole focus is to provide secure Internet SSO through identity federation to numerous applications and partners. These vendors provide best-of-breed functionality, and they will work with the identity management system you already have in place. These vendors should proactively go beyond the standards to address loopholes associated with underlying

technologies such as XML digital signatures and provide centralizing management and monitoring of security credentials and identity traffic.

5.3.9 Claims-Based Solutions

-Microsoft has developed a flexible claims architecture5 based on standard protocols such as WS-Federation, WS-Trust, and the Security Assertion Markup Language (SAML), which should replace today's more rigid systems based on a single point of truth, typically a directory of user information. The claims model can grow out of the infrastructure users have today, including Public Key Infrastructure (PKI), directory services, and provisioning systems. This approach supports the shared industry vision of an identity meta system that creates a single-user access model for any application or service and enables security-enhanced collaboration.

5.3.10 Identity-as-a-Service (IaaS)

-Identity-as-a-Service essentially leverages the SaaS model to solve the identity problem and provides for single sign-on for web applications, strong authentication, federation across boundaries, integration with internal identities and identity monitoring, compliance and management tools and services as appropriate. The more services you use in the cloud, the more you need IaaS, which should also include elements of governance, risk management, and compliance (GRC) as part of the service.

5.3.11 Compliance-as-a-Service (CaaS) provides

-Cost-effective multiregulation compliance verification
-Continuous audit
-Threat intelligence

5.3.12 The Future of Identity in the Cloud

-The challenges of managing identity in the cloud are far-reaching and include ensuring that multiple identities are kept secure. There must be coordination of identity information among various cloud services and among enterprise identity data stores and other cloud services. A flexible, user-centric identity management system is needed.

5.4 Privacy and Its Relation to Cloud-Based Information Systems

-The challenge in data privacy is to share data while protecting personally identifiable information.
-Privacy is an important business issue focused on ensuring that personal data is protected from unauthorized and inappropriate collection, use, and disclosure, ultimately preventing the loss of customer trust and inappropriate fraudulent activity such as identity theft, email spamming, and phishing.

5.4.1 Privacy Risks and the Cloud

-A user's privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by the cloud provider. For some types of information and some categories of cloud computing users, privacy and confidentiality rights, obligations, and status may change when a user discloses information to a cloud provider. Disclosure and remote storage may have adverse consequences for the legal status of or protections for personal or business information. The location of information in the cloud may have significant effects on the privacy and confidentiality protections of information and on the privacy obligations of those

who process or store the information. Information in the cloud may have more than one legal location at the same time, with differing legal consequences.

5.4.2 Protecting Privacy Information

-The Federal Trade Commission is educating consumers and businesses about the importance of personal information privacy, including the security of personal information. -In general, the basics for protecting data privacy are as follows, whether in a virtualized environment, the cloud, or on a static machine:

Collection: You should have a valid business purpose for developing applications and implementing systems that collect, use or transmit personal data.

Notice: There should be a clear statement to the data owner of a company's/providers intended collection, use, retention, disclosure, transfer, and protection of personal data.

Choice and consent: The data owner must provide clear and unambiguous consent to the collection, use, retention, disclosure, and protection of personal data.

Use: Once it is collected, personal data must only be used (including transfers to third parties) in accordance with the valid business purpose and as stated in the Notice.

Security: Appropriate security measures must be in place (e.g., encryption) to ensure the confidentiality, integrity, and authentication of personal data during transfer, storage, and use.

Access: Personal data must be available to the owner for review and update. Access to personal data must be restricted to relevant and authorized personnel.

Retention: A process must be in place to ensure that personal data is only retained for the period necessary to accomplish the intended business purpose or that which is required by law.

Disposal: The personal data must be disposed of in a secure and appropriate manner (i.e., using encryption disk erasure or paper shredders).

5.4.3 The Future of Privacy in the Cloud

-Robert Gellman for the World Privacy Forum, provides the following observations on he future of policy and confidentiality in the cloud computing environment: Responses to the privacy and confidentiality risks of cloud computing include better policies and practices by cloud providers, more vigilance by users, and changes to laws.
The cloud computing industry could establish standards that would help users to analyze the difference between cloud providers and to assess the risks that users face. Users should pay more attention to the consequences of using a cloud provider and, especially, to the provider's terms of service.

For those risks not addressable solely through policies and practices, changes in laws may be needed.

Users of cloud providers would benefit from greater transparency about the risks and consequences of cloud computing, from fairer and more standard terms, and from better legal protections. The cloud computing industry would also benefit.

6. Security in the Cloud

6.1 Chapter Overview

-To identify 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.

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.
-With the cloud model, you lose control over physical security. In a public cloud, you are sharing computing resources with other companies.
-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.
-If information is encrypted while passing through the cloud, who controls the encryption/decryption keys? Is it the customer or the cloud vendor?
-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.
-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.
-Cloud applications undergo constant feature additions, and users must keep up to date with application improvements to be sure they are protected.
-Having proper fail-over technology is a component of securing the cloud that is often overlooked. The company can survive if a non-missioncritical application goes offline, but this may not be true for mission-critical applications.
-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.
-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.
-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
-To establish zones of trust in the cloud, the virtual machines must be self-defending, effectively moving the perimeter to the virtual machine itself.

6.3. Software-as-a-Service Security

-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?

6.3.1 Security Management (People)

-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.

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.

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.

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.

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.

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.

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.

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.

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 tochanging threats.

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.
6.3.11 Third-Party Risk Management
-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
It is a 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.
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.
6.3.14 Forensics
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.
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. 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	4. Confidentiality	7. Privacy
2. Authorization	5. Integrity	
3. Availability	6. Accountability	

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.

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.

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.

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.

6.3.20 Data Privacy

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. The data governance framework should include:

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

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. True unified end-to-end security in the cloud will likely requires an ecosystem of partners

6.3.23 Application Security

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

6.3.24 Virtual Machine Security

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. Integrity monitoring and log inspection software must be applied at the virtual machine level.

6.3.25 Identity Access Management (IAM)

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. 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.

6.3.27 Physical Security

The key components of data center physical security are the following: Physical access control and monitoring, including 24/7/365 onsite 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 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.

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 rganization acceptance and maintenance.

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

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. 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 inhouse, 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.