Security in the Cloud

Chapter 11

Security in the Cloud

Unit Goals

- Provide a foundation for understanding security and risk.
- Apply basic security and risk concepts to the cloud.

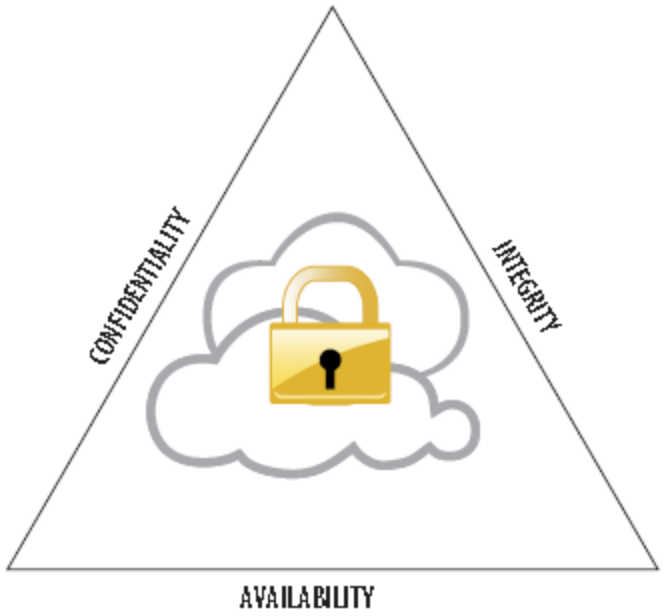

FIGURE 11.1 The CIA triad

Key Principles

Confidentiality

- Confidentiality refers to the sensitivity of data.
  - Confidential data needs to be protected from unauthorized access, use, or disclosure.

Integrity

- Integrity refers to the reliability of data.
  - To have integrity, data needs to be protected from unauthorized modification.

Availability

- Availability refers to the accessibility of data.
  - To be available, data needs to be protected from disruption of service.

Security Controls

- Security controls can be categorized as management, technical, or operational

Management

- Provides a framework for operational procedures.
  - Guidelines, standards, and policies.

Technical

- Applied directly to and executed by information technology resources.
  - Access control, authentication, firewalls, and encryption.

Operational

- Generally involve processes and procedures.
  - Based on management controls.
  - Incorporate technical controls.
  - Examples include disaster recovery planning, configuration management, incident response, and physical security.

Upper Management Support

- Management controls come from an organization's upper and executive management.
- It is their responsibility to set policy that supports business goals and to allocate resources in support of policy.
- Technical controls can be put into place by IT staff.
- Supervisors can implement operational controls.
- Critical security component.

Defense in Depth

- Layered framework that implement security controls on computing facilities, network perimeters, hosts (servers, workstations, laptops, and so on), applications, and data.

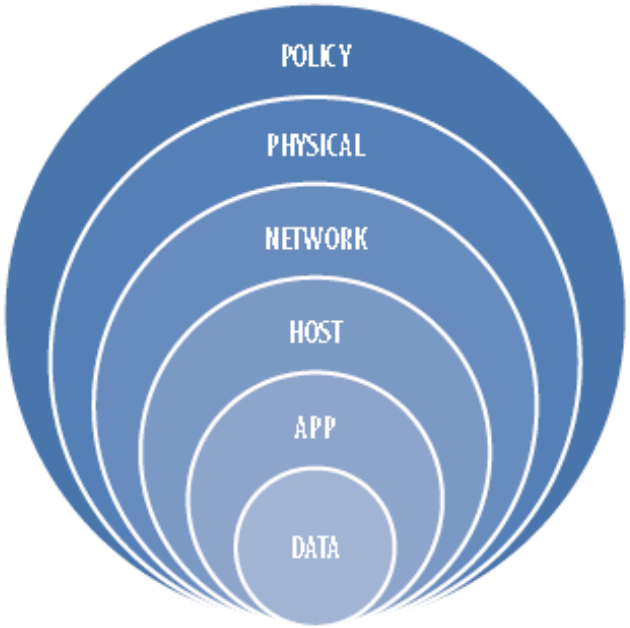

FIGURE 11.2 A layered security framework

Risk Management Basics

- Risk is a factor of probability (likelihood) and impact (loss)—specifically, the probability that a particular incident will occur and impact the business.

Incidents include:

- Theft or loss of equipment
- Unauthorized data access
- Denial of service
- Unauthorized data manipulation.

Risk Management Process

Step 1: Identify and categorize assets.

Step 2: Identify threats and vulnerabilities..

Step 3: Assess risk. (Document likelihood and cost.)

Step 4: Address risk. (Prioritize.)

Step 5: Monitor Risk Monitoring is performed to ensure that mitigation (or other risk management decisions) is effective.

More Risk Management

- ISO/IEC 31000 Risk Management Standard
- NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems
- COSO Enterprise Risk Management Integrated Framework

Reviewing Security Standards

- Standards are a set of established rules, principles, and requirements—an approved model.
  - The information security standard should be relative to organization's industry.

Information Security Standards

COBIT 5

- IT management and governance framework
  - Maintained by ISACA.

ISO/IEC 27000 series

- Information security management standards published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

NIST Special Publications – 800 series

- Standards generally suitable for organizations with comparable security requirements.
  - In some cases map directly to ISO/IEC standards.

Includes:

- SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing
- SP 800-145: The NIST Definition of Cloud Computing
- SP 800-146: Cloud Computing Synopsis and Recommendations

Open Security Architecture (OSA)

- An open-source project that provides security standards in the form of patterns, drawing from other recognized standards such as NIST SP 800-53.
- Cloud Computing Pattern (SP-011) identifies the key control areas and activities of cloud computing.

http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing

Payment Card Industry Data Security Standards (PCI-DSS)

- Maintained by PCI Security Standards Council
- Designed to protect cardholder data.
- Includes security requirements for:
  - Networking
  - data protection
  - vulnerability management
  - access control
  - Monitoring
  - policy.

Also includes specific requirements for shared hosting:

- Data and process isolation
- Logging and audit trails
- Timely forensic investigation

Exploring Common Security Risks and Mitigations

- Same basic risks apply to cloud computing.
  - In addition, cloud computing has its own risks.
  - Public and private clouds both require some type of security across boundaries.
- Cloud computing operates on a shared responsibility model, with organizations and providers having their own security-related duties.
- Before looking at specific risks and mitigation techniques, there are some perimeter defenses that should be implemented in all cloud implementations, where applicable.

Firewalls

- An appliance or application that inspects and regulates network traffic based on a set of rules.
  - Allows or blocks traffic on specific network ports or to/from specific hosts.
- Examinees data packets to identify the source, the destination, and sometimes the payload.
- Firewall appliances for use in a cloud computing environment have the ability to scale, are highly reliable with redundant network connections and power.
  - Generally more robust than traditional firewalls.

Virtual Firewalls

- Designed specifically to protect virtual hosts
  - Operates in different modes depending on how it is deployed.
- In bridge mode, the virtual firewall is deployed within the network infrastructure, where it acts like a traditional firewall.
- In hypervisor mode, the virtual firewall is not on the network at all but rather within the hypervisor environment in order to directly monitor virtual machine traffic.

Virtual Private Networks

- Secures private network that uses a public network (i.e., the Internet) or another intermediate network.
- VPN communications are isolated from the rest of the network through an IP tunnel
  - Secured through encryption and authentication.
- In cloud computing, allows end users to access cloud resources securely, regardless of location, as long as they have the proper credentials and are using a device that supports VPN client.

Application Interface

- Customers interact with cloud service providers through application programming interfaces (APIs).
- If APIs are not properly secured, it can impact all three elements of the CIA triad.
  - Data may be exposed or altered and services or accounts may be disabled or hijacked.
- APIs may be insecure due to weaknesses such as programming defects, transmission of data (including login credentials) in clear text, or ineffective monitoring.

Mitigation Against Weak APIs

- Generally responsibility of provider.
- Adequate testing particularly important when APIs interact with each other.
- Some responsibilities may be shared, such as authentication and access control and the use of encryption for communications.
- If necessary, requirements should be in the SLA.

Shared Technology

- A benefit of cloud computing is economy of scale due to shared resources and multitenancy.
  - Shared technology also creates vulnerabilities.
- In a multitenant environment, availability may be impacted by performance issues caused by improper allocation of storage or memory or even by attacks against another customer.
- Confidentiality or integrity may be impacted by insufficient data isolation.

Two Shared Technology Mitigations

1. Operational security
2. Incident response.

Operational security processes include:

- Application of proper controls
- Timely testing and installation of security patches

Security monitoring.

- A provider should have a defined process for responding to security breaches and notifying customers.

Insider and Criminal Threats

- Malicious insiders may find employment with a cloud service provider.
- Pose risk to legitimate customers because they may be sharing resources that could be blacklisted or involved in criminal investigation.
- As mentioned earlier, accounts may be hijacked due to vulnerabilities in APIs.
- Accounts as well as network traffic and even the service itself may be compromised through hacking, phishing, password theft, and other criminal tactics.

Mitigation

- Cloud service providers can mitigate the risk of malicious insiders doing damage by implementing HR processes such as background and reference checks as well as strong internal security policies and controls.
- For example, access for provider employees should follow the principle of least privilege and employee actions should be logged in audit trails.

Data Exposure and Loss

- Risks also include weak authentication and access control, insecure deletion of data, and jurisdictional issues.
- Data loss can occur during normal operations as the result of a system failure or due to a security incident.

Mitigation

- Encryption of data in storage and transmission mitigates risk of unauthorized data access.
- Encryption can also be used in user authentication.
- Implementing symmetric encryption requires key management.
  - Key management encompasses the life cycle of a key, from initial generation to eventual revocation.
  - It also includes processes to securely exchange, store, and replace keys.
  - Lost keys can render data unreadable, and compromised keys may lead to loss of data confidentiality or integrity.
- Other mitigations include strong authentication and access control, periodic auditing, secure deletion of data, and appropriate disaster recovery planning.

Organizational Risks

- The organization itself is also exposed to security risks by implementing cloud services.
- Foremost is the loss of control, particularly when hybrid or public clouds are used.
- In all service models (e.g., IaaS, PaaS, SaaS), customers cede a significant amount of control to the cloud service provider, often with very little transparency with regard to security controls, hiring practices, location, and general business practices.

Mitigation

- SLA should clearly define security responsibilities of both organization and service provider.
  - Other elements addressable in the SLA include, but are not limited to, security incident notification procedures, recovery time, and the right to audit.
  - Once cloud services are adopted, security policies should be updated to reflect new processes and procedures associated with the cloud environment as well as acceptable use of cloud services.
- Once security policies have been developed and approved, organizational staff must be educated through a security awareness training program.
- Threats are managed through an information security management system (ISMS), which is, generally speaking, a system of policies, processes, and controls.
- ISMS implementations are based on the Plan-Do-Check-Act (PDCA) process. PDCA, as illustrated in Figure 11.6, is an iterative cyclical management process.

FIGURE 11.6 The PDCA cycle

Plan: Design the system.

- The organization identifies the security standards and policies that apply to its environment, defines security metrics, and uses risk assessment results to identify appropriate security controls.

Do: Implement the controls.

- Controls selected as a result of the risk assessment implemented.

Check: Evaluate system.

- Includes, but is not limited to, monitoring logs, analyzing metrics, and review-ing assessment results.

Act: Change as necessary.

- Changes to the ISMS will need to be made periodically.
  - Due to the identification of changes in regulation or security policy, changes to the computing environment, or identification of vulnerabilities and opportunities for improvement.

Responding to Incidents

- An incident is any event that impacts the confidentiality, integrity, or availability of an information system, including unplanned interruptions of service.
- Incidents are not limited to malicious attacks against a system.
- Also include events such as accidental information releases, power or network failures, and theft or loss of computing equipment.

Incident Management

- Process of planning for, detecting, and responding to incidents.
  - aka incident response.
- An incident response plan includes step-by-step instructions for the incident response process.
  - Not all incidents trigger formal incident response.
- Incident response team (IRT) is a trained group of individuals prepared and authorized to handle incidents.
  - Team should include qualified technical personnel, upper management, and representatives from various organizational units such as human resources, legal, and public relations.
- Responsibility shared between cloud service provider and customer.

Incidents

Cloud service provider and the customer must have clear understanding of:

- What constitutes an incident
- Cloud service provider's incident response capabilities
- Communication procedures between the customer's incident response team and the provider's incident response team
- Recovery requirements and capabilities
- Any legal considerations, particularly with regard to data ownership and jurisdiction

Incident Response Considerations

- Incident response discussions should occur prior to vendor selection.
- Both customer and provider roles and responsibilities should be clearly outlined in the SLA.

Digital Forensics in the Cloud

- Digital investigations often requires digital forensics.
- The forensic process involves acquiring the devices to be analyzed, performing the analysis on a forensic image of the device's media, and generating a report.
- In traditional computing, if forensic analysis were required, the physical server would be seized and imaged.
- In a public cloud computing environment, everything is virtualized and evidence can reside on multiple virtual and physical servers, none of which are owned by the data owner and all of which have multiple tenants whose privacy must be respected.
- Additional complications occur if the cloud service provider's network crosses geopolitical boundaries.

Forensic Dependencies

- Organizations that are concerned about being able to successfully perform digital forensic investigations should investigate using cloud service providers that have adequate tools and procedures available to support investigation and are willing to provide access to such via the SLA.
- Organizations would also be wise to consider the number of dependencies involved because cloud service providers often purchase services from other cloud service providers and each dependency adds additional complexity.

Recognizing Security Benefits

- Cloud service providers have the ability to take advantage of economy of scale.
- Can potentially provide a greater level of security than an organization could on its own by spreading the cost out across its customer base.

Includes:

- Increased availability and improved disaster recovery through redundancy and multiple locations
- Security specialists
- 24/7 staffing and monitoring

- When evaluating cloud services, as well as individual providers, an organization must take into account the security capabilities of the provider versus its own security capabilities.

Questions???