IT Service Delivery And Support Week Eleven - Info. Security

IT Auditing and Cyber Security

Fall 2016

Instructor: Liang Yao

IT Service Delivery and Support

* Information Security
  * **Recent Security Incidents**
  * **Security Objectives**
  * **Security Process**
  * **Governance**
  * **Information Security Risk Assessment**
  * **Information Security Strategy**
  * **Security Controls Implementation**
  * **Security Monitoring**

IT Service Delivery and Support

Top 10 2012 Security Incidents

* **# 10. Wyndham Hotels –**
  * **credit card information were stored in plain text**
  * **Data was stolen THREE times in two years**
  * **Over 600,000 credit card numbers fell into the wrong hands**
  * **$10.5 billion in fraudulent transactions was reported**
  * **Gaining attention from the Federal Trade Commission**
* **# 9. Yahoo**
  * **More than 400,000 plaintext Yahoo passwords were posted on the Internet on July 11th**
  * **the "Tech-Company-Shoulda-Known-Better" factor**
  * **SQL Injection**

IT Service Delivery and Support

* #8. Apple
  * A million Apple Unique Identifiers (UDIDs) were released by "AntiSec"
  * The group claims to have 11 million more UDIDs
  * Leveraged a Java vulnerability to access authentication related information
  * To embarrass FBI, which was in the midst of investigating the hacktivist group Anonymous.
* # 7. Global Payments
  * Theft of about 1.5 million credit cards
  * Include Track 2 data – can be used to clone credit cards
  * names, addresses and social security numbers were apparently not breached
  * Impact merchants and consumers

IT Service Delivery and Support

* # 6. Ghostshell
  * 1.6 million government and contract accounts were posted to Pastebin records by "Team Ghostshell"
  * Involving aerospace, the defense industry, financial services and law enforcement
  * Stolen data included names, email addresses, passwords, phone numbers and various forms of administrator account information.
  * "ProjectWhiteFox"- intended to attract support for freedom of information on the Internet.
* # 5. LinkedIn
  * 6.5 million Linkedin passwords (compromised of "unsalted SHA-1 hashes)
  * Passwords were published in various places on the Web
  * Team effort to crack the passwords

IT Service Delivery and Support

* **4. Nationwide Insurance, Allied Insurance Companies**
  * **PII information breach -** 1.1 million customers and applicants
  * including names, Social Security numbers, driver's license numbers, date of birth and possibly marital status, gender, occupation and employment information
  * No Medical information and credit card numbers
  * High value of the information

* **3. South Carolina**
  * Approximately 3.8 million tax records and nearly 400,000 credit card numbers were stolen from the South Carolina Department of Revenue.
  * Over 2 million incidents of information theft were also nabbed through the same spearphishing exploit that stole employee usernames and passwords to gain access to the sensitive data.
  * Improper password policies and failure to encrypt social security numbers were key enablers of the operation
  * It's believed to be the largest data theft from a state government.

IT Service Delivery and Support

* **#2. Zappos**
  * **Personal details on 24 million people were hacked and stolen**
  * **Information Including** names, home addresses, email addresses, phone numbers, the last four digits of credit card numbers, and passwords
  * The company stepped up with a highly proactive response that involved new passwords and increased numbers of call center folks to help victims navigate the situation.

* 1. The Biggest Breach Of 2012: The Government Sector

  * Government sector, which, according to Boston-based security vendor Rapid7, has reported 268 individual data breaches over a period of roughly three years.
  * In all, governments reportedly exposed more than 94 million records containing personally identifiable information.
  * The data reveals that the number of breaches has continued to escalate each year since 2009. And, it's expected that the likely tally for 2012 will actually double the number from 2011.
  * In addition to hacking incidents, the numbers include unintended disclosure, the loss or theft of portable devices and physical loss of devices.

Security Objectives

* Availability-The ongoing availability of systems addresses the processes, policies, and controls used to ensure authorized users have prompt access to information. This objective protects against intentional or accidental attempts to deny legitimate users access to information or systems.

* Integrity of Data or Systems-System and data integrity relate to the processes, policies, and controls used to ensure information has not been altered in an unauthorized manner and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.

* *Underlying Models for IT Security, NIST, SP800-33, p. 2*

Security Objectives (Cont.)

* Confidentiality of Data or Systems-Confidentiality covers the processes, policies, and controls employed to protect information of customers and the institution against unauthorized access or use.

* Accountability-Clear accountability involves the processes, policies, and controls necessary to trace actions to their source. Accountability directly supports nonrepudiation, deterrence, intrusion prevention, security monitoring, recovery, and legal admissibility of records.

* Assurance-Assurance addresses the processes, policies, and controls used to develop confidence that technical and operational security measures work as intended. Assurance levels are part of the system design and include availability, integrity, confidentiality, and accountability. Assurance highlights the notion that secure systems provide the intended functionality while preventing undesired actions.

Information Security Processes

* Information Security Risk Assessment-A process to identify and assess threats, vulnerabilities, attacks, probabilities of occurrence, and outcomes.
* Information Security Strategy-A plan to mitigate risk that integrates technology, policies, procedures, and training. The plan should be reviewed and approved by the board of directors.
* Security Controls Implementation-The acquisition and operation of technology, the specific assignment of duties and responsibilities to managers and staff, the deployment of risk-appropriate controls, and the assurance that management and staff understand their responsibilities and have the knowledge, skills, and motivation necessary to fulfill their duties.

Information Security Processes (Cont.)

* Security Monitoring-The use of various methodologies to gain assurance that risks are appropriately assessed and mitigated. These methodologies should verify that significant controls are effective and performing as intended.
* Security Process Monitoring and Updating-The process of continuously gathering and analyzing information regarding new threats and vulnerabilities, actual attacks on the institution or others combined with the effectiveness of the existing security controls. This information is used to update the risk assessment, strategy, and controls. Monitoring and updating makes the process continuous instead of a onetime event.
* Security risk variables include threats, vulnerabilities, attack techniques, the expected frequency of attacks, financial institution operations and technology, and the financial institution's defensive posture. All of these variables change constantly. Therefore, an institution's management of the risks requires an ongoing process.

Governance

* Management Structure

  “Information security is a significant business risk that demand engagement of the Board of Directors and senior business management. It is the responsibility of everyone who has the opportunity to control or report the institution's data. Information security should be supported throughout the institution, including the board of directors, senior management, information security officers, employees, auditors, service providers, and contractors. Each role has different responsibilities for information security and each individual should be accountable for his or her actions. Accountability requires clear lines of reporting, clear communication of expectations, and the delegation and judicious use of appropriate authority to bring about appropriate compliance with the institution's policies, standards, and procedures.” FFIEC IT Examination Handbook

Governance

* **Responsibility and Accountability**
  * Board
  * Executive Management
  * Staff and Line-of-Business Managers
  * Internal Auditors

Governance (Cont.)

* Board
  * Central oversight and coordination,
  * Assignment of responsibility,
  * Risk assessment and measurement,
  * Monitoring and testing,
  * Reporting, and
  * Acceptable residual risk.

Governance (Cont.)

* Senior Management (security)
  * Clearly support all aspects of the information security program;
  * Implement the information security program as approved by the board of directors; Establish appropriate policies, procedures, and controls; Participate in assessing the effect of security issues on the financial institution and its business lines and processes;
  * Delineate clear lines of responsibility and accountability for information security risk management decisions;
  * Define risk measurement definitions and criteria;
  * Establish acceptable levels of information security risks; and
  * Oversee risk mitigation activities.

Governance (Cont.)

* Senior Management (Integrity)
  * Ensure the security process is governed by organizational policies and practices that are consistently applied,
  * Require that data with similar criticality and sensitivity characteristics be protected consistently regardless of where in the organization it resides,
  * Enforce compliance with the security program in a balanced and consistent manner across the organization,
  * Coordinate information security with physical security, and
  * Ensure an effective information security awareness program has been implemented Information Security Booklet throughout the organization.

Governance (Cont.)

* Staff & Line Managers
  * Contribute to design and implementation of IT activities
  * Review and monitor security controls
  * Define security requirements
* Internal Auditors
  * Assess information control environments, including understanding, adoption and effectiveness
  * Validate IS efforts and compare current practices to industry standards
  * Recommend improvement

Information Security Risk Assessment

Key Steps

* Gather Necessary Information
* Identification of Information and Information Systems
* Analyze the Information
  * Classify and Rank Sensitive Data, Systems, and Applications
  * Assess Threats and Vulnerabilities
  * Evaluate Control Effectiveness
* Assign Risk Ratings

Information Security Risk Assessment

Key Risk Assessment Practices

* Multidisciplinary and Knowledge Based Approach
* Systematic and Central Control
* Integrated Process
* Accountable Activities
* Documentation
* Enhanced Knowledge
* Regular Updates

Information Security Strategy

Architecture Considerations

* Control Objectives for Information and Related Technology (CobiT) - provides a broad and deep framework for controls.
* IT Infrastructure Library (ITIL) - provides a list of recognized practices for IT service management.
* ISO 17799 - provides a library of possible controls that can be included in an architecture and guidance in control selection.
* BITS (Bank Information Technology Secretariat) and other industry publications for discrete controls, such as vendor management.

Information Security Strategy

IS Policies and Procedures

* Implementing through ordinary means, such as system administration procedures and acceptable-use policies;
* Enforcing policy through security tools and sanctions;
* Delineating the areas of responsibility for users, administrators, and managers;
* Communicating in a clear, understandable manner to all concerned;
* Obtaining employee certification that they have read and understood the policy;
* Providing flexibility to address changes in the environment; and
* Conducting annually a review and approval by the board of directors.

Information Security Strategy

* **Technology Design**
* **Outsourced Security Services**

Security Controls Implementation

Access Control

* Access Rights Administration
* Shared Secret Systems
* Token Systems
* Public Key Infrastructure
* Encryption
* Authenticator Reissuance
* Behavioral Authentication
* Device Authentication
* Mutual Authentication
* Authentication for Single Sign-On Protocols

Security Controls Implementation

Examples of Common Authentication Weaknesses, Attacks, and Offsetting Controls:

* Dictionary and brute force
* Warehouse attacks, (compromise an entire authentication mechanism)
* Social engineering
* Client attacks (password, PKI key, etc.)
* Replay attacks
* Man-in-the-middle attacks, and
* Hijacking

Security Controls Implementation

* **Network Access**
  * **Layers of Access Control**
    * Group network servers, applications, data, and users into security domains (e.g., untrusted external networks, external service providers, or various internal user systems);
    * Establish appropriate access requirements within and between each security domain;
    * Implement appropriate technological controls to meet those access requirements consistently; and
    * Monitor cross-domain access for security policy violations and anomalous activity.

Security Controls Implementation

* **Network Access**
  * **Network configuration considerations**
    * Identifying the various applications and systems accessed via the network
    * Identifying all access points to the network including various telecommunications channels (e.g., wireless, Ethernet, frame relay, dedicated lines, remote dial-up access, extranets, Internet)
    * Mapping the internal and external connectivity between various network segments
    * Defining minimum access requirements for network services (i.e., most often referenced as a network services access policy)
    * Determining the most appropriate network configuration to ensure adequate security and performance

Security Controls Implementation

* **Firewalls -** (**NIST Special Publication 800-41, "Guidelines on Firewalls and Firewall Policy." is a collection of components (computers, routers, and software) that mediate access between different security domains.)
* **Types of Firewalls**
  * Packet Filter Firewalls
  * Stateful Firewalls
  * Application Firewalls

Security Controls Implementation

Firewall Policy

* Firewall topology and architecture
* Type of firewall(s) being utilized
* Physical placement of the firewall components
* Monitoring firewall traffic
* Permissible traffic (generally based on the premise that all traffic not expressly allowed is denied, detailing which applications can traverse the firewall and under what exact circumstances such activities can take place)
* Firewall updating
* Coordination with security monitoring and intrusion response mechanisms
* Responsibility for monitoring and enforcing the firewall policy, Protocols and applications permitted
* Regular auditing of a firewall's configuration and testing of the firewall's effectiveness
* Contingency planning

Security Controls Implementation

Other Network Access Related Concerns:

* Malicious Code Filtering
* Outbound Filtering
* Network Intrusion Prevention Systems
* Quarantine
* DNS Placement

Security Controls Implementation

Wireless Issues

* Treating wireless networks as untrusted networks, allowing access through protective devices similar to those used to shield the internal network from the Internet environment
* Using end-to-end encryption in addition to the encryption provided by the wireless connection
* Using strong authentication and configuration controls at the access point and on all clients
* Using an application server and dumb terminals
* Shielding the area in which the wireless LAN operates to protect against stray emissions and signal interference
* Monitoring and responding to unauthorized wireless access points and clients

Security Controls Implementation

Remote Access

* Disallow remote access by policy and practice unless a compelling business justification exists
* Require management approval for remote access
* Regularly review remote access approvals and rescind those that no longer have a compelling business justification
* Appropriately configure remote access devices.
* Appropriately secure remote access devices against malware (see "Malicious Code Prevention")

Security Controls Implementation

Remote Access

* Appropriately and in a timely manner patch, update, and maintain all software on remote access devices
* Use encryption to protect communications between the access device and the institution and to protect sensitive data residing on the access device
* Periodically audit the access device configurations and patch levels
* Use VLANs, network segments, directories, and other techniques to restrict remote access to authorized network areas and applications within the institution

Security Controls Implementation

Remote Access

Implement controls consistent with the sensitivity of remote use. For example, remote use to administer sensitive systems or databases may include the following controls:

* Restrict the use of the access device by policy and configuration;
* Require two-factor user authentication
* Require authentication of the access device
* Ascertain the trustworthiness of the access device before granting access
* Log and review all activities (e.g. keystrokes)

Security Controls Implementation

Remote Access

* If remote access is through modems:
  * Require an operator to leave the modems unplugged or disabled by default, to enable modems only for specific and authorized external requests, and disable the modem immediately when the requested purpose is completed
  * Configure modems not to answer inbound calls, if modems are for outbound use only
  * Use automated callback features so the modems only call one number (although this is subject to call forwarding schemes)
  * Install a modem bank where the outside number to the modems uses a different prefix than internal numbers and does not respond to incoming calls

Security Controls Implementation

Remote Access

* Log remote access communications, analyze them in a timely manner, and follow up on anomalies
* Centralize modem and Internet access to provide a consistent authentication process, and to subject the inbound and outbound network traffic to appropriate perimeter protections and network monitoring
* Log and monitor the date, time, user, user location, duration, and purpose for all remote access
* Require a two-factor authentication process for remote access (e.g., PIN-based token card with a one-time random password generator, or token-based PKI)

Security Monitoring

* Architecture Issues
* Activity Monitoring

Security Monitoring

Architecture Issues

* Network traffic policies that address the allowed communications between computers or groups of computers
* Security domains that implement the policies
* Sensor placement to identify policy violations and anomalous traffic
* The nature and extent of logging
* Log storage and protection, and
* Ability to implement additional sensors on an ad hoc basis.

Security Monitoring

* **Activity Monitoring**
  * Network Intrusion Detection Systems
  * Honeypots
  * Host Intrusion Detection Systems
  * Log Transmission, Normalization, Storage, and Protection
* **Condition Monitoring**
  * Self Assessments
  * Metrics
  * Independent Tests

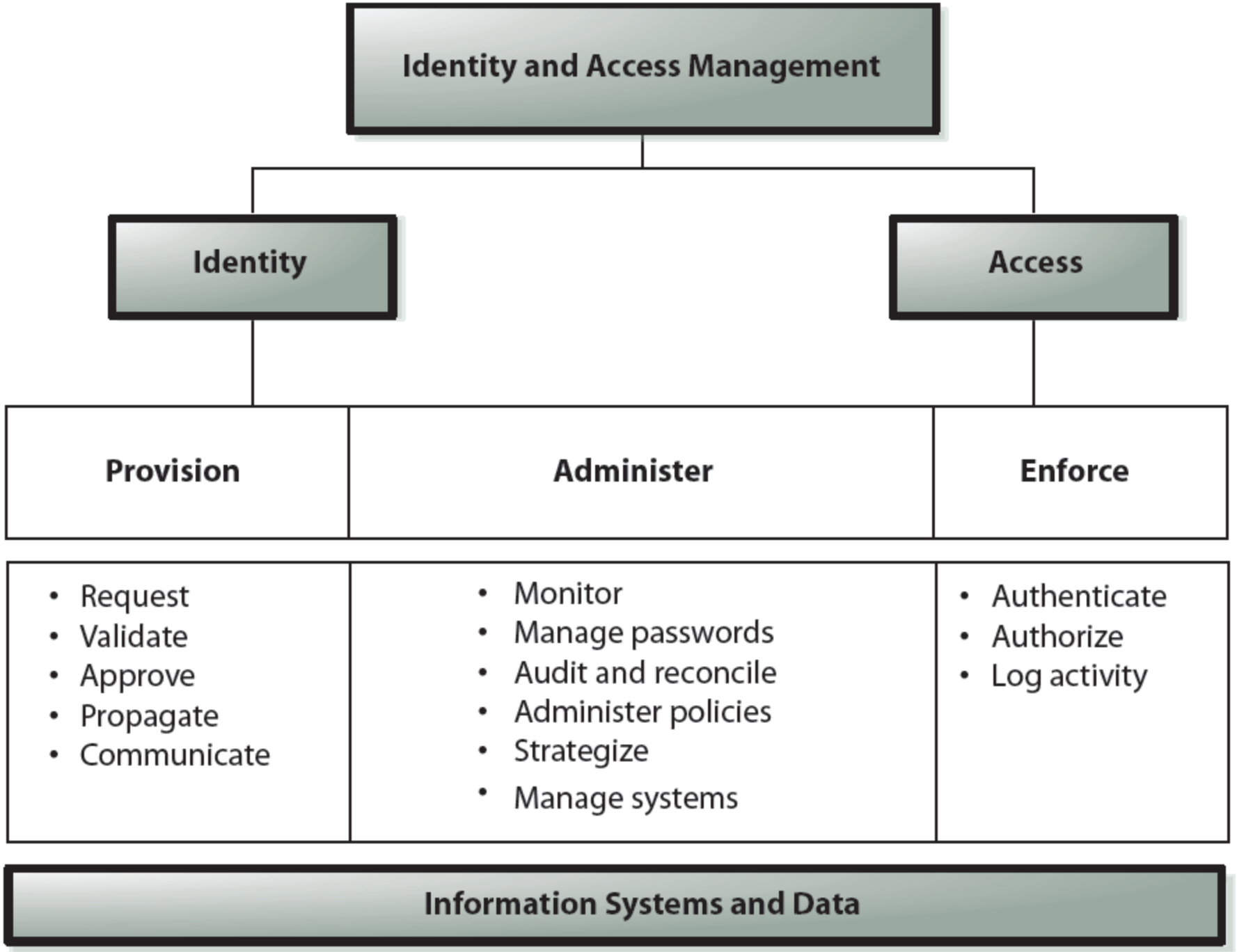

Figure 1. Relationships between IAM components and key concepts

Policy, Planning, Politics, and Management

80 %

20 %

Technology

Define the business architecture

Define functional/business requirements

Review & update po

$

Define budget

Q1 '07

Q4 '10

Define timeline

Identif regula

Hardware/ software

Storage

Access management

Application integration