



الجامعة السعودية الإلكترونية
SAUDI ELECTRONIC UNIVERSITY
2011-1432

Bachelor of Science in
Information Technology
IT409
IT Security and Policies

Security Program and Policies

Principles and Practices

by Sari Stern Greene
Updated 02/2018



*Chapter 8: Communications and
Operations Security*



Objectives

- Author useful standard operating procedures
- Implement change control processes
- Understand the importance of patch management
- Protect information systems against malware
- Consider data backup and replication strategies
- Recognize the security requirements of email and email systems
- Appreciate the value of log data and analysis
- Evaluate service provider relationships
- Write policies and procedures to support operational and communications security



Introduction

- Communication and operations security focuses on Information technology (IT) and Security functions:
 - Standard operating procedures
 - Change management
 - Malware protection
 - Data replication
 - Secure management
 - Activity monitoring
- These functions are carried out by IT and information security data custodians (e.g. network administrations security engineers)



Standard Operating Procedures (SOPs)

- SOPs are detailed explanations of how to perform a task
- SOPs provide; standardized direction, improved communication, reduced training time and improved work consistency
- Effective SOPS include:
 - Who performs the task
 - What materials are necessary
 - Where the task takes place
 - When the task should be performed
 - How the person is to execute the task



SOPs Documentation

- SOPs should be properly documented to protect the company
 - A critical task/business process is only known by one employee and is not documented, if that employee becomes unavailable, the organization could be seriously injured
- Documented SOPs standardize the target process and provide sufficient information
 - someone with limited experience can successfully perform the procedure unsupervised
- SOPs should be written in detail by someone with sufficient experience of the targeted process



Authorizing SOP Documentation

- Documented procedure must be:
 - Reviewed
 - The reviewer should check the SOP for clarity and reliability
 - Verified
 - The verifier should test the procedure and ensure they are correct and not missing any steps
 - Authorized (before publication)
 - The process owner is responsible for authorization, publication and distribution of the document



Protecting SOP Documentation

The integrity of the SOP document should be protected through:

- **Access controls**

- Should be applied to protect the procedure document from any tampering

- **Version controls**

- Employees should use the latest revision of the procedure



Developing SOPs

- SOPs should be:
 - Concise & clear
 - Logical step-by-step order
 - Plain language format
 - Exceptions are noted and explained
 - Warnings are clear and standout
- Choosing the format of a SOP is based on:
 - How many decisions the user will make
 - How many steps are in the procedure



Developing SOPs

- There are four common SOP formats:
 - Simple step
 - Procedure contains less than 10 steps
 - Does not involve many decisions
 - Hierarchical/Graphic
 - Procedure contains more than 10 steps
 - Does not involve many decisions
 - Flowchart
 - Procedure can contain any number of steps
 - Involves many decisions



Developing SOPs

TABLE 8.1 SOP Methods

Many Decisions?	More Than Ten Steps?	Recommended SOP Format
No	No	Simple Step
No	Yes	Hierarchical or Graphic
Yes	No	Flowchart
Yes	Yes	Flowchart



Developing SOPs

TABLE 8.2 Simple Step Format

Procedure	Completed
	<p>Note: These procedures are to be completed by the night operator by 6:00 a.m., Monday–Friday. Please initial each completed step.</p>
1. Remove backup tape from tape drive.	
2. Label with the date.	
3. Place tape in tape case and lock.	
4. Call ABC delivery at 888-555-1212.	
5. Tell ABC that the delivery is ready to be picked up.	
6. When ABC arrives, require driver to present identification.	
7. Note in pickup log the driver's name.	
8. Have the driver sign and date the log.	



Developing SOPs

TABLE 8.3 Hierarchical Format

New User Account Creation Procedure

Note: You must have the HR New User Authorization Form before starting this process.

Procedures	Detail
Launch Active Directory Users and Computers (ADUC).	a. Click on the TS icon located on the administrative desktop. b. Provide your login credentials. c. Click the ADUC icon.
Create a new user.	a. Right-click the Users OU folder. b. Choose New User.
Enter the required user information.	a. Enter user first, last, and full name. b. Enter user login name and click Next. c. Enter user's temporary password. d. Choose User Must Change Password at Next Login and click Next.
Create an Exchange mailbox.	a. Make sure Create an Exchange Mailbox is checked. b. Accept the defaults and click Next.



Developing SOPs

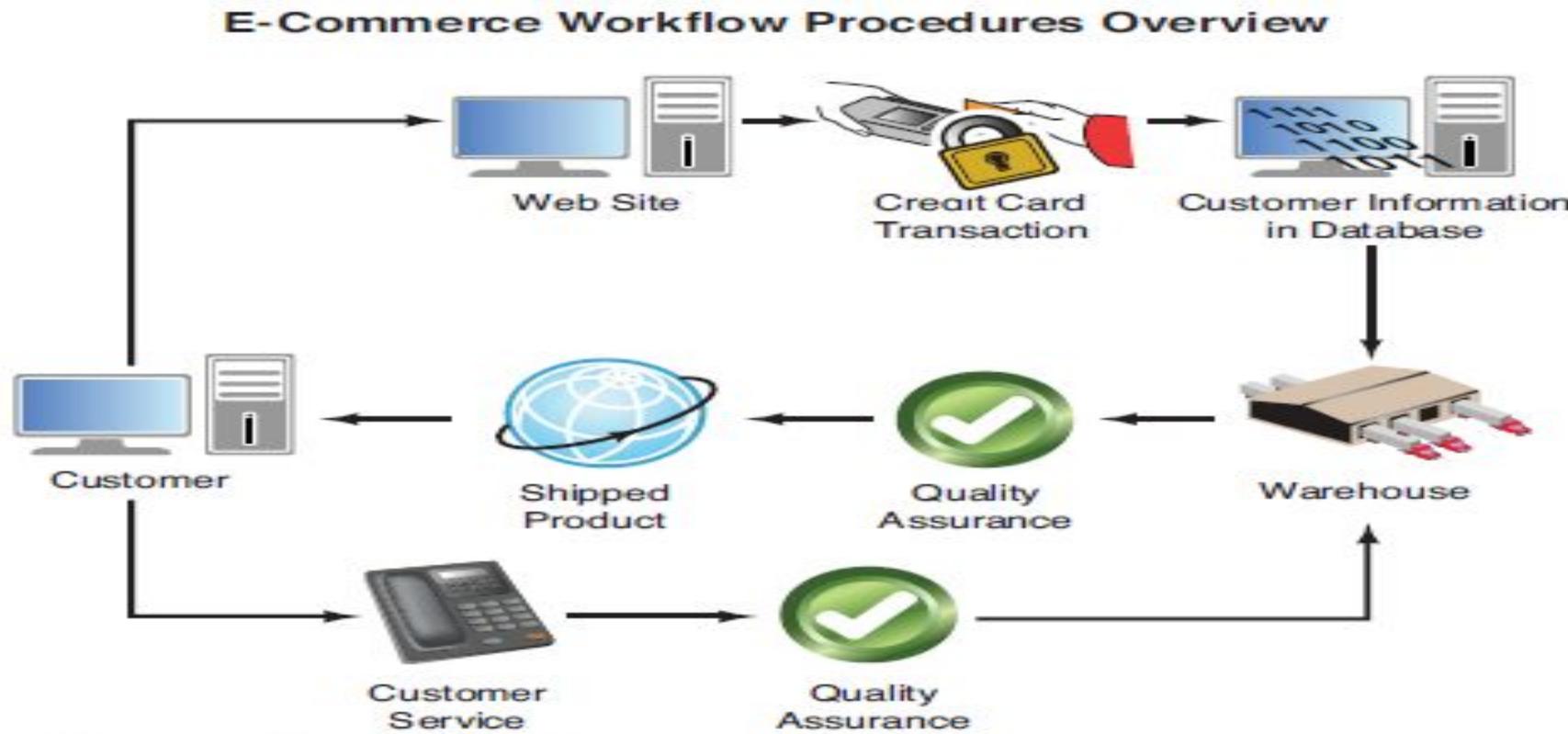


FIGURE 8.1 Example of the graphic format.



Developing SOPs

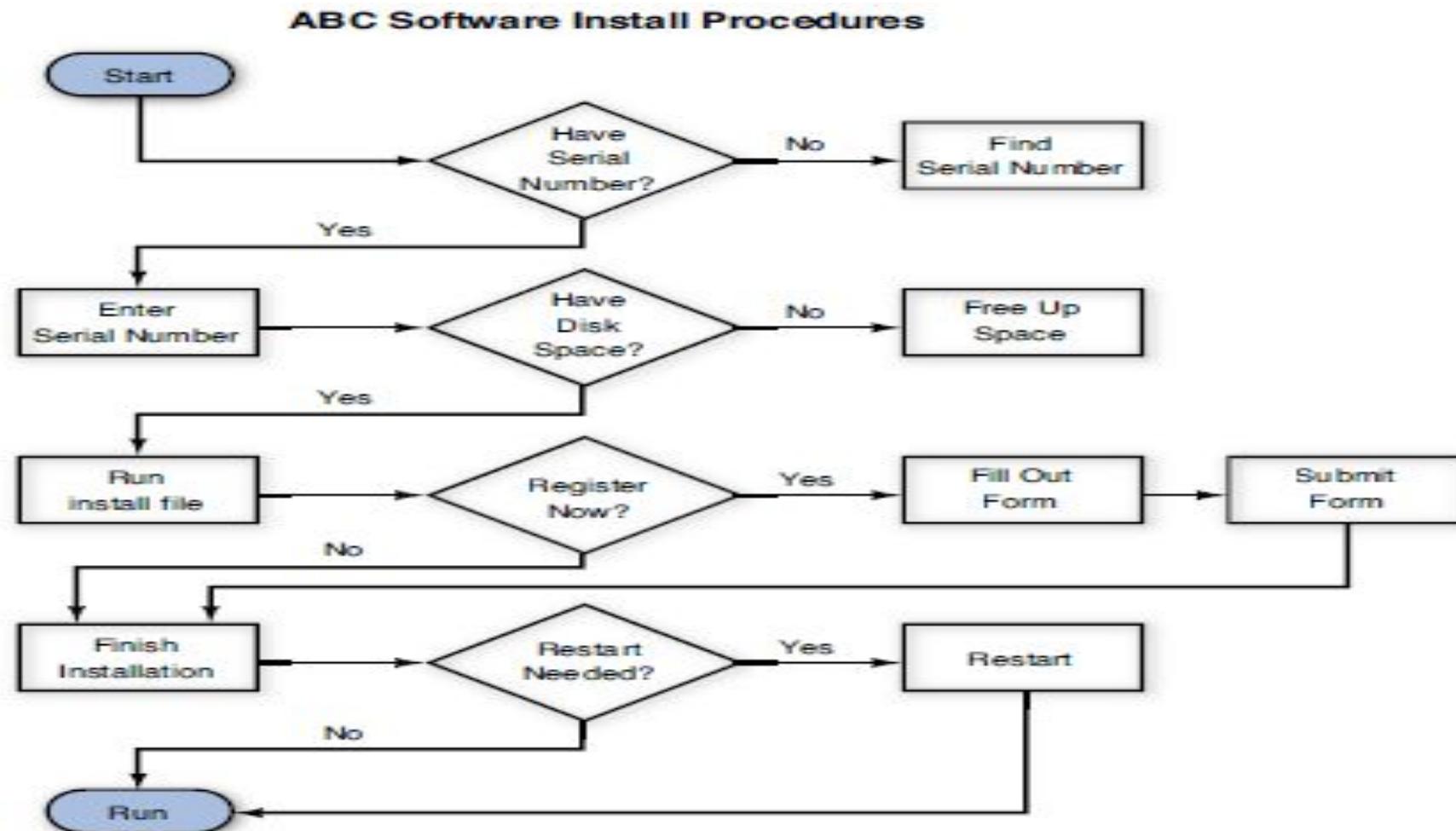


FIGURE 8.2 Flowchart format.



Operational Change Control

- **Change control:**
 - An internal procedure in which authorized changes are made.
- Managing change allows organizations to be productive and spend less time in crisis mode.
 - E.g. An operating system fails to be updated completely to the new version nor is it still original version, this results in an unstable platform hindering the productivity of the entire company



Operational Change Control

- **The change control process:**

1. Submitting a Request For Change (RFC)
2. Developing a change control plan
3. Communicating change
4. Implementing & monitoring change



Submitting a Request for Change

- The first phase of the change control process is an RFC submission
- **The RFC should include:**
 - Description of the proposed change
 - Justification why the change should be implemented
 - Impact of not implementing the change
 - Alternatives
 - Cost
 - Resource requirements and timeframe
- **The change is then evaluated and if approved implemented**



Developing a Change Control Plan

- Once the change is approved, the next step is to develop a change control plan
- The change control plan should include:
 - Security reviews to ensure no new vulnerabilities are introduced
 - Implementation instructions
 - Rollback and/or recovery options
 - Post implementation monitoring
- The complexity of the change and its risk to the organization will influence the level of detail within the change control plan.



Communicating Change

- Change must be communicated to all relevant parties
- There are two main categories of messages that are communicated:
 - **Messages about the change, which should include:**
 - Current situation
 - The need for change
 - What the change is, how it will change and when
 - **Messages how the change will impact employees**
 - Impact on day-to-day activities of the employees
 - Implication on job security



Implementing & Monitoring Change

- Change can be unpredictable
 - If possible change should be applied to a test environment to check and monitor its impact.
 - A plan must be in place to roll back or recover from failed implementation
- All actions and steps taken to implement the change should be recorded and documented
- Change should be continuously monitored for any flaws and unexpected impacts



Why Is Patching Handled Differently?

- Patch is software or code designed to fix a problem
- Applying security patches is the primary method of fixing security vulnerabilities in software
- Patches need to be applied quickly to prevent attackers from exploiting code and information
- Patch management is the process of scheduling, testing, approving, and applying security patches
 - Patching can be unpredictable and disruptive
 - User should be notified of potential downtime due to patch installation



Malware Protection

- Malware (malicious software) is designed to:
 - disrupt computer operation
 - gather sensitive information
 - or gain unauthorized access to computer systems and mobile devices
- Malware can infect system by being bundled with other programs or self-replicated
- Most malware typically requires user interaction such as:
 - Clicking an email
 - Connecting to the internet



Different Types of Malware

- Malware can be categorized as:
 - Viruses: malicious code that attaches to become part of another program
 - Worm: a piece of code that spreads from one computer to another without requiring a host file
 - Trojans: malicious code that masks itself as an application
 - Bots: Snippets of code designed to automate tasks and respond to instructions



Different Types of Malware Cont.

- Malware can be categorized as:
 - Ransomware: a type of malware that take computer or its data as hostage
 - Rootkits: a set of software tools that hides its presence on the computer, using some of the lower layers of the operating system
 - Spyware/adware: general term describing software that tracks internet activity and searches without user knowledge



How Is Malware Controlled?

- Prevention controls
 - Stop an attack before it occurs
 - Disable remote desktop connection
 - Configure the firewall to restrict access
 - Disallow users to install software on company device
- Detection controls
 - Identify the presence of malware, alert the user, and prevent the malware from carrying out its mission
 - Real-time firewall detection of suspicious files download and of suspicious network connections



What Is Antivirus Software?

- Antivirus software is used to detect, contain, and in some cases eliminate malicious software
- Most AV software employs two techniques
 - Signature-based recognition
 - Behavior-based (heuristic) recognition
- AV software is not 100% effective due to three factors
 - The volume of new malware
 - Single-instance malware
 - Blended threats (malware put together)



Data Replication

- The impact of malware, hardware failure, accidental deletion is reduced by effective:
 - Data Replication
 - is the process of copying data to a second location that is available for immediate use
 - Data backup
 - is the process of copying/storing data that can be restored to its original location
- Replicating and backing up data protects data's integrity and availability



Recommended Backup/Replication Strategy?

- Decision to backup/replicate and how often should be based on the impact of not being able to access the data
- Several factors should be considered when the strategy is designed:
 - Reliability
 - Speed and efficiency
 - Simplicity and ease of use
 - Cost
- Backed-up or replicated data should be stored in a off-site location, secure from theft, the elements, and natural disasters



The Importance of Testing

- The point of replicating and backing-up data is so the data can be accessed/restored if lost or tampered with
- The accessibility or restore strategy must be:
 - Carefully designed
 - Tested before being approved
 - Documented



Secure Messaging

- Emails take complex routes with processing and sorting at several locations before arriving at its destination
 - It's hard to tell if someone has read or manipulated your message in transit making it an insecure way to transmit information
- Conserving the confidentiality of the content and metadata of a message is extremely difficult
- Email can be used to distribute malware
- Encryption protects the privacy of the message by converting it from readable plain text to ciphers text



Securing Messaging Cont.

- Sent document may contain metadata that the sender didn't intend to share
- Metadata are hidden information about a file:
 - Creator of the document
 - Deleted, reformatted or hidden content
- Recycling documents, using documents created by other people can be ways in which metadata is shared



Securing Messaging Cont.

- Email is an effective way to spread malware and attack/infiltrate organizations
- Malware is spread in emails through:
 - Attachments
 - Hyperlinks
 - Email hoax: Email containing false information (such as virus warnings) asking user to perform actions that can be damaging
- Email users and employees should:
 - Be careful of attachments, hyperlinks and spam emails
 - Not access personal email accounts from corporate networks



Securing Messaging Cont.

Common e-mail-related mistakes are:

- Hitting the wrong button
 - using “reply all” as instead of “reply” or “forward” instead of “reply”
- Sending an e-mail to the wrong e-mail address
 - Sending to the wrong address because it is close to the intended recipient’s address (especially with the use of autocomplete addresses)
- Forwarding an email with the entire string
 - Leaving a third person with information discussed in earlier e-mails that should have been private



Are E-Mail Servers at Risk?

- Email servers are hosts that deliver, forward, store emails
- Compromising the e-mail server can happen by:
 - Relay abuse: using mail servers to distribute spam/malware
 - DDoS attack: an attack against the availability of the email service
- Blacklisting is used to deny emails coming from a specified IP address, domain name or email address that is known for spam/malware.



Activity Monitoring and Log Analysis

- Logs are used to record events occurring within an organization's systems and networks
- Log management activities include:
 - Configure log sources, log generations, storage & security
 - Perform analysis of log data
 - Initiate appropriate responses to identified events
 - Manage the long-term storage of log data
- Data logs should be selected based on their ability to:
 - identify suspicious activity and attacks
 - help understand normal activity
 - provide operational oversight
 - provide a record of activity



Analyzing Logs

- Data log analysis can be a reliable way to discover, potential threats, malicious activity and provide operational oversight
- Log analysis techniques include:
 - Correlation: ties individual log entries together based on related information
 - Sequencing: examines activity based on patterns
 - Signature: compares log data to “known bad” activity
 - Trend analysis: identifies activity overtime that alone might seem normal



Service Provider Oversight

- Companies may outsource aspects of their operations, introducing vulnerabilities
- CIA requirements must extend to all service providers who store, process, transmit, or access information on company systems
- Due diligence is a process used to assess adequacy of service providers and is documentation of:
 - Corporate history and financial status
 - Qualifications and backgrounds etc.
- Even if the due diligence documentation (SSAE16- most common) is done and approved, ongoing monitoring should be continued



Summary

- Day-to-day activities can have a huge impact on the security of the network and the data it contains. SOPs are important in providing a consistent framework across the company.
- Change must be managed. Two mandatory components of a change management process are RFC documents and a change control plan.
- Malware is becoming the tool of choice for criminals to exploit devices, operating systems, applications, and user vulnerabilities. Many types of malware exist and companies should protect against them.
- Sound backup strategies should be developed, tested, authorized and implemented. E-mail, while being a fantastic business tool, is also a double-edge sword because of its inherent lack of built-in security and must be treated as such.
- Operational security extends to service providers. Service provider controls should meet or exceed those of the company.



Thank You



Security Program and Policies

Principles and Practices

by Sari Stern Greene
Updated 02/2018



Objectives

- Understand the rationale for the systems development lifecycle (SDLC)
- Recognize the stages of software releases
- Appreciate the importance of developing secure code
- Be aware of the most common application development security faults
- Explain cryptographic components
- Develop policies related to systems acquisition, development, and maintenance



System Security Requirements

- Security must be taken into account from the genesis of the project
- Retroactively attempting to inject security back into existing code usually either does not work or ends up creating new vulnerabilities and/or instability in the code



What Is SDLC?

- Systems development lifecycle (SDLC) provides a standard process for any system development
- There are five phases in the SDLC according to NIST
 1. Initiation phase
 - Establishes the need for a system and documents its purpose
 2. Development /acquisition phase
 - The system is designed, purchased, programmed, or developed



What Is SDLC? Cont.

- There are five phases in the SDLC according to NIST

3. Implementation phase

- The system is tested and retested, and any modifications are applied until it is accepted

4. Operational phase

- The system is put into production-should include monitoring, auditing, testing

5. Disposal phase

- Ensure the orderly termination of the system



What Is SDLC? Cont.

Initiation phase

- Security planning starts here.
- Information system is evaluated for security requirements,
- Project managers and developers must consider the security implications while taking decisions, throughout the development
- Other tasks: assignment of roles and responsibilities, identification of compliance requirements, security metrics, etc.,



What Is SDLC? Cont.

Development / acquisition phase

- **Conduct risk assessment** and use it to design the base security controls.
- **Risk assessment is iterative**, Whenever new functionality is added, risk assessment should be done.
- **Security controls must be tested** to ensure that they perform as intended.



What Is SDLC? Cont.

Implementation phase

- Test the functionalities of the security features.
- Design reviews and system testing must be done before placing the system for operation
- Final task is authorization- by the designee or system owner- this process is known as certification and accreditation (C&A)
- The authorization officials depend on security plan, risk assessment reports and test results.



What Is SDLC? Cont.

Operational / maintenance phase

- System is in operation. If any enhancement to software/hardware can be developed and tested.
- Configuration management and change control processes are done (need for any change and how to do it).
- Periodic testing and evaluation
- New vulnerabilities must be fixed, until that the system may go offline



What Is SDLC? Cont.

Disposal phase

- No retirement age for code!!
- System normally evolve from one generation to another, based on changing requirements /improvements.
- If there is a need for discarding the system, it should be done without affecting the protected or confidential data. Disposal must be done according to the disposal policy of the organization.



What Is SDLC? Cont.

- SDLC principles apply to commercial off-the-shelf software (COTS) and open source software
 - Development is not done in-house but should be evaluated to ensure it meets or exceeds the organization's security requirement
 - Only stable and tested software should be deployed



What Is SDLC? Cont.

- Software Releases
 - Alpha phase
 - Initial release of software for testing
 - Can be unstable
 - Beta phase
 - Software is complete and ready for usability testing
 - Release candidate (RC)
 - Hybrid of beta and final release version
 - Has the potential of being final release unless significant issues are identified
 - General availability or go live
 - Software has been made commercially available



What Is SDLC? Cont.

▪ Software Updates

- Updates are different from security **patches**
- Security patches are designed to address a specific vulnerability
- Updates include functional enhancements and new features
- Updates should be thoroughly tested
- A documented **rollback** strategy should exists before applying any updates
- If update required a system reboot, it should be delayed until the reboot has the least impact on business operations



What Is SDLC? Cont.

- Testing Environment Concerns

- Companies SHOULD have a test environment
- The closer to the live environment the test environment is, the more expensive it is, but the more accurate the testing will be
- The cost of setting up the test environment should be compared to the cost of a loss of data confidentiality, integrity, and/or availability because of a patch-related reason
- Testing environment should be 100% segregated from the live network
- Live data should NEVER be used in a test environment
- The test servers may not be as well secured as the live, production servers
- De-identified or dummy data should be used in place of live data



Secure Code

- Two types of code
 - Insecure code (referred as “sloppy code”)
 - Secure code
 - Deploying secure code is responsibility of the systems’ owner
- The Open Web Application Security Project (OWASP)
 - Open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted
 - Every 3 years releases the top 10 most critical web application security flaws



Secure Code Cont.

- Injection
- Input validation
- Dynamic data verification
- Output validation
- Broken authentication and session management



Secure Code Cont.

- **Injection**
 - OWASP defines injection as when untrusted data is sent to an interpreter as part of a command or query.
 - The attacker's hostile data can trick the interpreter into executing an unintended command or accessing data without proper authorization.
 - Preventing injection requires keeping untrusted data separate from commands and queries.



Secure Code Cont.

- **Input validation**
 - Input validation is the process of validating all the input to an application before using it. This includes correct syntax, length, characters, and ranges.
 - The objective of input validation is to evaluate the format of entered information and, when appropriate, deny the input.
 - Input validation would look at how many and what type of characters are entered in the field. This strategy is known as whitelist or positive validation.



Secure Code Cont.

- Dynamic data verification
 - Dynamic data is defined as **data that changes as updates become available**—for example, an e-commerce application that automatically calculates sales tax based on the ZIP Code entered.
 - The process of checking that the sales tax rate entered is indeed the one that matches the state entered by the customer is another form of input validation.



Secure Code Cont.

- **Output validation**
 - Output validation is the process of validating (and in some cases, masking) the output of a process before it is provided to the recipient.
 - An example would be substituting asterisks for numbers on a credit card receipt.
 - Output validation controls what information is exposed or provided.



Secure Code Cont.

- Broken authentication and session management
 - Number two on the 2013 and 2017 OWASP list is broken authentication and session management.
 - If session management assets such as user credentials and session IDs are not properly protected, the session can be hijacked or taken over by a malicious intruder.
 - A critical security design requirement must be strong authentication and session management controls.
 - A common control for protecting authentication credentials and session IDs is encryption.



Cryptography

- **Cryptography:** The process that takes plain text and turns it into ciphertext
- **Encryption** is the conversion of plain text into what is known as cipher text using an algorithm called a cipher.
- **Decryption**, the inverse of encryption, is the process of turning cipher text back into readable plain text.
- **Ciphertext:** Text that cannot be read unless you apply the correct algorithm and predetermined value
- The predetermined value is also referred to as a **key**
- The **key** must be securely stored and strong enough to resist brute force cracking attempts



Cryptography Cont.

- Hashing
 - The process of creating a numeric value that represents the original text
 - It is a one-way process
 - Provides integrity but not confidentiality and authentication
- Digital signature:
 - A hash value that has been encrypted with the sender's private key
 - Insures nonrepudiation and data integrity
 - Does not insure data confidentiality



Cryptography Cont.

- Symmetric key
 - Uses a single secret key that must be shared in advance and kept private
- Asymmetric key
 - Also known as public key
 - Uses two different but mathematically related keys
 - One is called public and the other one private



Cryptography Cont.

Public Key Infrastructure (PKI)

- Framework and services used to create, distribute, manage, and revoke public keys
- Components
 - Certification Authority (CA)
 - – issues and maintains Digital certificates
 - Registration Authority (RA)
 - performs the administrative functions, including verifying the identity of users and organizations requesting a digital certificate, renewing certificates, and revoking certificates



Cryptography Cont.

Public Key Infrastructure (PKI)

- Components

- Client nodes
 - interfaces to users
- Digital certificate
 - contains public key of certificate holder, serial number, name, validity period, name of certificate issuer, digital signature, algorithm id.



Cryptography Cont.

- Protecting the encryption keys
- Compromised keys mean that the confidential data is not safe anymore
- Worse if the company does not know that the key has been compromised as it will continue to rely on it and use it to send confidential data, thinking that it is secure
- Someone must be officially responsible for the security of the keys
 - Usually, it is a senior IT employee, in correlation with the information security officer



Cryptography Cont.

- Digital certificates can be revoked

- Usually a bad sign! It means there is a chance that the key has been compromised
- If there's the slightest chance that a key may have been compromised, the digital certificate MUST be revoked
- Revocation lists are kept to verify that a given certificate has not been revoked
- Certificates can be suspended when it is known that it won't be used for a period of time
- Key destruction must occur before a hard drive is reused



Summary

- Data availability needs are at an all-time high. Custom applications must be created with security in mind from the start of the project, which includes a **risk assessment** and proper **input and output validation**, along with regular security tests.
- **Patching** a server is not a trivial task and should be accomplished according to the patch management policy.





الجامعة السعودية الإلكترونية
SAUDI ELECTRONIC UNIVERSITY
2011-1432

Bachelor of Science in
Information Technology
IT409
IT Security and Policies

Security Program and Policies

Principles and Practices

by Sari Stern Greene
Updated 02/2018



Objectives

- Define the relationship between information security and personnel practices
- Recognize the stages of the employee lifecycle
- Describe the purpose of confidentiality and acceptable use agreements
- Understand appropriate security education, training, and awareness programs
- Create personnel-related security policies and procedures



Introduction

- Employees need access to information and information systems.
- Thus, we must know our employees' background, education, and weaknesses.
- Before employees are given access to information and information systems:
 - They must understand organizational expectations, policies, handling standards, and consequences of noncompliance.
 - This information is generally codified into two agreements:
 1. a confidentiality agreement
 2. an acceptable use agreement

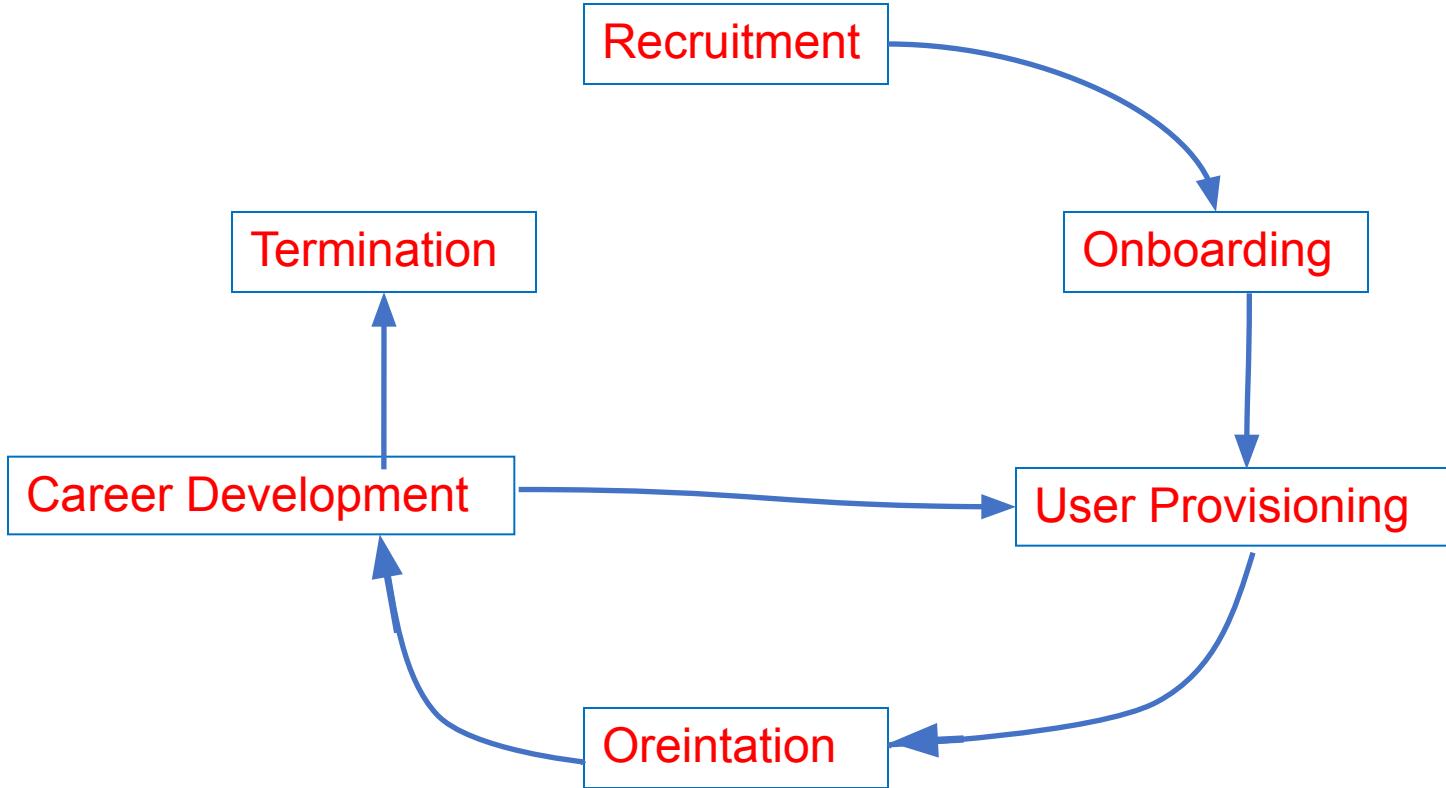


The Employee Lifecycle

- Represents stages in the employee's career
- Lifecycle models can vary but most include the following stages:
 1. Recruitment
 2. Onboarding
 3. User provisioning
 4. Orientation
 5. Career development
 6. Termination



The Employee Lifecycle (Cont.)



The Employee Lifecycle (Cont.)

1. Recruitment:

It includes all the processes leading up to and including the hiring of a new employee.

2. Onboarding:

The employee is added to the organization's payroll and benefits systems.



The Employee Lifecycle (Cont.)

3. User provisioning:

The employee is assigned equipment as well as physical and technical access permissions.

- It is also invoked whenever there is a change in the employee's position, level of access required, or termination.



The Employee Lifecycle (Cont.)

4. Orientation:

The employee settles into the job, integrates with the corporate culture, familiarizes himself with coworkers and management, and establishes his role within the organization.

5. Career development:

The employee matures in his role in the organization. Professional development frequently means a change in roles and responsibilities.



The Employee Lifecycle (Cont.)

6. Termination:

The employee leaves the organization.

- processes are somewhat dependent on whether the departure is the result of resignation, firing, or retirement.
- Tasks include removing the employee from the payroll and benefits system, recovering information assets such as his smartphone, and deleting or disabling user accounts and access permissions.



What Does Recruitment Have to Do with Security?

- Risks and rewards of posting online employment ads:
 - A company can reach a wider audience
 - A company can publish an ad that gives too much information:
 - About the network infrastructure and therefore allow a hacker to **footprint** the internal network easily and stealthily
 - About the company itself, inviting **social engineering attacks**



Job Postings

- Job descriptions are supposed to:
 - Convey the mission of the organization
 - Describe the position in general terms
 - Outline the responsibilities attached to said position
 - Outline the company's commitment to security via the use of such terms as **non-disclosure agreement**



Job Postings

- Job descriptions are NOT supposed to:
 - Include information about specific systems, software versions, security configurations, or access controls
 - It's harder to hack a network if one doesn't know what hardware & software
 - If the above information is deemed necessary, two versions of the position can be created. The second, more detailed version should be posted internally and shared with candidates that have made the “first cut”



Candidate Application Data

- Companies are responsible for protecting the data and privacy of the job seeker
- Non-public personal information (NPPI) should not be collected if possible



The Interview

- Job Interview:
 - The interviewer should be concerned about revealing too much about the company during the interview
 - Job candidates should **never gain access** to secured areas
 - A job interview is a perfect foot-printing opportunity for hackers and social engineers



Screening Prospective Employees

- An organization should protect itself by running extensive **background checks** on potential employees at all levels of the hierarchy
- Some higher level positions may require even more in-depth checks
- Many U.S. government jobs require prospective employees have the requisite clearance level



Types of Background Checks

- The company should have a basic background check level to which all employees are subjected.
- Not all potential employees need to undergo the same level of scrutiny
- Information owners may require more in-depth checks for specific roles.



Types of Background Checks

- Rules that need to be considered when conducting background checks:
 1. Workers' right to privacy:
 - Not all information is fair game to gather.
 - Workers have a right to privacy in certain personal matters.
 - Only information relevant to the actual work they perform.



Types of Background Checks

2. Getting consent:

- Companies should seek **consent** from employees before launching a background check.
- consent request needs to be included on the application forms and requires the applicant to agree in writing.

3. Using social media:

- Social media sites are increasingly being used to “learn more” about a candidate.
- In some countries, law prohibits the use of this information for hiring



Types of Background Checks Cont.

- Educational records fall under FERPA (Family Educational Rights and Privacy Act). Schools must first have written authorization before they can provide student-related information
- Motor vehicle records fall under DPPA (Drivers Privacy Protection Act), which means that the DMV – or its employees – are not allowed to disclose information obtained by the department
- The FTC allows the use of credit reports prior to hiring employees as long as companies do so in accordance with the Fair Credit Reporting Act



Types of Background Checks Cont.

- Bankruptcies may not be used as the SOLE reason to not hire someone according to Title 11 of the U.S. Bankruptcy Code
- Criminal history: The use of this sort of information varies from state to state
- Worker's compensation records: In most states, these records are public records, but their use may not violate the Americans with Disabilities Act



Types of Background Checks Cont.

TABLE 6.1 Types of Background Checks

Check Type	Description
Educational	Verification that all educational credentials listed on the application, resume, or cover letter are valid and have been awarded.
Employment	Verification of all relevant previous employment as listed on the application, resume, or cover letter.
License/certification	Verification of all relevant licenses, certifications, or credentials.
Credit history	Checking the credit history of the selected applicant or employee. Federal laws prohibit discrimination against an applicant or employee because of bankruptcy. Federal law also requires that applicants be notified if their credit history influences the employment decision.
Criminal history	Verification that the selected applicant or employee does not have any undisclosed criminal history.



What Happens in the Onboarding Phase?

- The new hire is added to the organization's payroll and benefit systems
- New employees must provide
 - Proof of identity
 - Work authorization
 - Tax identification
- Two forms that must be completed
 - Form I-9
 - Form W-4



What Is User Provisioning?

- The process of:
 - Creating **user accounts** and group memberships
 - Providing company identification
 - Assigning access **rights** and **permissions**
 - Assigning access devices such as tokens and/or smartcards
- The user should be provided with and acknowledge the terms and conditions of the **Acceptable Use Agreement** before being granted access



What Should an Employee Learn During Orientation?

- His responsibilities
- Information handling standards and privacy protocols
- Ask questions



Why Is Termination Considered the Most Dangerous Phase?

- The terminated employee may seek revenge, create havoc, or take information with him.
- How to handle termination properly:
 - Disable access to the network, internal, and web-based application, email, and company owned social media.



The Importance of Employee Agreements

- Confidentiality or non-disclosure agreements
 - Agreement between employees and organization
 - Defines what information may not be disclosed by employees
 - Goal: To protect sensitive information
 - Especially important in these situations:
 - When an employee is terminated or leaves
 - When a third-party contractor was employed



The Importance of Employee Agreements cont.

- **Acceptable Use Agreement**
 - A policy contract between the company and information systems user
- Components of an Acceptable Use Agreement
 - Introduction
 - Data classifications
 - Applicable policy statement
 - Handling standards
 - Contacts
 - Sanctions for violations
 - acknowledgment



The Importance of Employee Agreements cont.

- Components of an Acceptable Use Agreement
 1. **Introduction** -sets the tone for the agreement and emphasizes the commitment of the leadership of the organization.
 2. **Data classifications** define (and include examples of) the classification schema adopted by the organization.



The Importance of Employee Agreements cont.

- Components of an Acceptable Use Agreement
 - 3. Applicable policy statement include Authentications & Password Controls, Application Security, Messaging Security (including email, instant message, text, and video conferencing), Internet Access Security, Remote Access Security, Mobile Device Security, Physical Access Security, Social Media, Incident Use of Information Resources, Expectation of Privacy, and Termination.



The Importance of Employee Agreements cont.

- Components of an Acceptable Use Agreement
 - 5. **Handling standards** dictate by classification level how information must be stored, transmitted, communicated, accessed, retained, and destroyed.
 - 6. **Contacts** should include to whom to address questions, report suspected security incidents, and report security violations.
 - 7. **The Sanctions for Violations** section details the internal process for violation as well as applicable civil and criminal penalties for which the employee could be liable.
 - 8. **The Acknowledgment** states that the user has read the agreement, understands the agreement and the consequences of violation, and agrees to abide by the policies presented. The agreement should be dated, signed, and included in the employee permanent record.



The Importance of Security Education and Training

- Training employees
 - According to NIST: “Federal agencies [...] cannot protect [...] information [...] without ensuring that all people involved [...]:
 - Understand their role and responsibilities related to the organization’s mission
 - Understand the organization’s IT security policy, procedures and practices
 - Have at least adequate knowledge of the various management, operational and technical controls required and available to protect the IT resources for which they are responsible”



The Importance of Security Education and Training cont.

- Hackers adapt: If it is easier to use social engineering – i.e., targeting users – rather than hack a network device, that is the road they will take
- Only securing network devices and neglecting to train users on information security topics is ignoring half of the threats against the company



What Is the SETA Model?

- What is SETA?
 - Security Education Training and Awareness.
1. Awareness:
 - It is not training; It is focusing the attention of employees on security topics to change their behavior.
 - Intended to allow individuals to recognize IT security concerns and respond accordingly.
 - Security awareness programs are designed to remind the user of appropriate behaviors.
 - A poster reminding employee to check and make sure the door is shut completely is an example of an awareness program.



What Is the SETA Model?

2. Security training:

- “seeks to teach skills” (per NIST).
- Examples:
 - training a firewall administrator how to close ports.
 - training an auditor how to read logs.
- Security training should NOT be dispensed only to the technical staff but to all employees.



What Is the SETA Model?

3. Security Education

- Per NIST: The ‘Education’ level integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles (technological and social), and strives to produce IT security specialists and professionals capable of vision and pro-active response.
- Security training should NOT be dispensed only to the technical staff but to all employees.



What Is the SETA Model?

3. Security Education, Cont.

- Education is generally targeted to those who are involved in:
 - the decision-making process.
 - classifying information.
 - choosing controls.
 - evaluating and reevaluating security strategies



What Is the SETA Model? Cont.

TABLE 6.2 NIST SP 800-16 SETA Model

Security	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	Awareness
Teaching Method	Discussion, seminar, reading	Lecture, case study, hands on	Interactive, video, posters, games
Test Measure	Essay	Problem solving	True or false, multiple choice
Impact Timeframe	Long-term	Intermediate	Short term



Summary

- A security policy that does not include personnel as a permanent threat to the data owned by the company is incomplete. Social engineering is more virulent than ever.
- Failing to train users on security topics is a bad mistake and may result in a lack of compliance for some federal mandates.
- All users should sign the Acceptable Use Agreement before receiving access to company's systems and equipment.



Thank You





الجامعة السعودية الإلكترونية
SAUDI ELECTRONIC UNIVERSITY
2011-1432

Bachelor of Science in
Information Technology
IT409
IT Security and Policies

Security Program and Policies

Principles and Practices

by Sari Stern Greene
Updated 02/2018



Objectives

- Define the concept of **physical security** and how it relates to information security
- Evaluate the security requirements of **facilities, offices, and equipment**
- Understand the **environmental risks** posed to physical structures, areas within those structures, and equipment
- Enumerate the **vulnerabilities** related to reusing and disposing of equipment
- Recognize the risk posed by the **loss or theft** of mobile devices and media
- Develop policies designed to ensure the **physical environmental security** of information, information systems, and information processing and storage facilities



Introduction

- ISO 27002:2013 encompasses both physical and environmental security.
- Environmental security refers to the workplace environment, which includes the design and construction of the facilities, how and where people move, where equipment is stored, how the equipment is secured, and protection from natural and man-made disasters.
- A physical security expert may question the location, the topography, and even the traffic patterns of pedestrians, automobiles, and airplanes.

Creating and maintaining physical and environmental security is a team effort.



Introduction

- Security professionals often focus on **technical** controls and can overlook the importance of **physical** controls
- Early Computer Age (Easy system protection):
 - Locked labs, heavy computers and only few were granted access to information
- Today:
 - Transportable computers, many employees/workers and limited privacy



Understanding the Secure Facility Layered Defense Model

- If an intruder bypasses one layer of controls, the next layer should provide additional defense and detection capabilities
- Both physical and psychological
 - The appearance of security is deterrent
 - E.g. Medieval castles:
 - built of stone, on a high hill, with guards, and one entry way
 - all designed to ward off intruders.



How to Secure the Site

- Physical protection is required for information-processing facilities:
 - A closet of one server
 - A complex of buildings with thousands of computers
- In addressing site physical security, we must consider:
 - Theft
 - Malicious destruction
 - Accidental damage
 - Damage that results from **natural disasters**



How to Secure the Site cont.

- The design of a secure site starts with the **location**
- Evaluating location-based threats:
 - Political stability
 - Susceptibility to terrorism
 - Crime rate in the area
 - Roadways and flight paths
 - Utility stability
 - Vulnerability to natural disasters
- Critical information processing facilities should be **inconspicuous** and **unremarkable**



How to Secure the Site Cont.

- The physical perimeter can be protected using:
 1. Obstacles:
 - Berms, Fences, Gates, and Bollards
 - Illuminated entrances, exits, pathways, and parking areas
 2. Detection systems:
 - Cameras, closed-circuit TV, alarms, motion sensors, and security guards
 3. Response system:
 - Locking gates and doors, personnel notification and direct communication with police



How Is Physical Access Controlled?

- **Physical entry and exit controls:**

Depending on the site and level of security required, available access controls (camera, locks, etc.) can be selected from

- Authorizing Entry (building access)
- Securing Offices, Rooms, and Facilities (within the building)
- Working in Secure Areas
- Ensuring clear desks and screens



Authorizing Entry

- Access control rules should be designed for:
 - Employees
 - Third-party (contractors/partners/vendors)
 - Visitors
- Physical entry/access controls (rules):
 - Authorized users should be authorized prior to gaining access to protected area
 - Visitors should be **identified, labeled, and authorized** prior to gaining access to protected area



Authorizing Entry cont.

- Physical entry/access controls (rules):
 - Visitors should be required to wear **identification** that can be evaluated from a distance, such as a **badge**
 - Identification should start as soon as a person attempts to gain entry



Securing Offices, Rooms, and Facilities

- Workspaces should be classified based on the **level of protection required**
 - Some internal rooms and offices as well as parts of individual rooms (cabinets and closets) may also require different levels of protection
- Classification system should address
 - Personnel security
 - Information system security
 - Documents security



Securing Offices, Rooms, and Facilities

- Secure design controls for spaces within a building include (but are not limited to) the following:
 - Structural protection such as full height walls, fireproof ceilings, and restricted vent access
 - Alarmed solid, fireproof, lockable, and observable doors
 - Alarmed locking, unbreakable windows
 - Monitored and recorded entry controls (keypad, biometric, card swipe)
 - Monitored and recorded activity



Working in Secure Areas

- It is not enough to just physically secure an area but, close attention should be paid to
 - who is allowed to access the area
 - what they are allowed to do
- The area should be
 - continually monitored
 - access control lists should be review frequently
- Based on the circumstances, devices are restricted from entering certain areas
 - cameras, smartphones, tablets, and USB drives



Ensuring Clear Desks and Screens

- Companies have a responsibilities to protect physical and digital information (during the workday and non-business hours)
- Protected or confidential documents should never be viewable to unauthorized personnel
 - Document should be locked in file rooms, desk drawers and cabinets when not in use
 - Copiers, scanners, and fax machines should be located in nonpublic areas and require the use of codes



Ensuring Clear Desks and Screens

- Unauthorized access can be the result of viewing a document left unattended
- Also protect documents or screens from **Shoulder Surfing**
- Shoulder surfing, is the act of looking over someone's shoulder to see what is displayed on a monitor or device.
- **Password-protected** screen savers should be **automated** to engage automatically.
- Users should be **trained** to lock their screens when leaving devices unattended.
- Physical security expectations and requirements should be included in organizational **acceptable use agreements**.



Protecting Equipment (No Power, No Processing?)

- No power, no processing—it's that simple
- All information systems rely on **clean, consistent, and abundant** supplies of electrical power.
- **Portable devices** that run on battery power require electricity for replenishment.
- **Power is not free.**
- Quite the contrary: Power can be very expensive, and excessive use has an environmental and geopolitical impact



Protecting Equipment (Energy Consumption)

- After lighting, computers and monitors have the **highest energy consumption** in office environments.
- As power consumption and **costs rise**, saving energy is becoming a significant issue
- **Universities** and Fortune 500 organizations have been leaders in the sustainable “green” computing movement.
- The goals of sustainable computing are to
 - **Reduce the use of hazardous materials,**
 - **Maximize energy efficiency** during the product’s lifetime,
 - **Promote the recyclability** or biodegradability of defunct products and factory waste.



Protecting Equipment

- Both company and employee-owned equipment should be protected
- To function **properly**, systems need **consistent power delivered at the correct voltage level**.
- Systems need to be protected from **power loss**, **power degradation**, and even from **too much power**, all of which can damage equipment.



Protecting Equipment

- Common causes of voltage variation include:
- Lightning; damage to overhead lines from storms, trees, birds, or animals; vehicles striking poles or equipment; and load changes or equipment failure on the network.
- Heat waves can also contribute to power interruptions as the demand in electricity
- The variation may be minor or significant.



Protecting Equipment

- Hardware assets must be protected from:
 - Power surges: Prolonged increase in voltage
 - Power spikes: momentary increase in voltage
 - Blackouts: Prolonged periods of power loss
 - Fault: momentary loss of power
 - Sag: Momentary periods of low voltage
 - Brownout: Prolonged period of low voltage



Protecting Equipment Cont.

- Protective devices can be installed to help protect the area and assets such as
 - Voltage regulators
 - Isolation transformers
 - Line filters
- No power, No processing
 - Reduce power consumption, for example by purchasing Energy Star certified devices



How Dangerous Is Fire?

Three elements of fire protection:

1. Fire prevention controls

- These are the first line of defense.
- Fire prevention controls include:
 - hazard assessments and inspections,
 - adhering to building and construction codes,
 - using flame-retardant materials, and
 - proper handling and storage procedures for flammable/combustible materials.



How Dangerous Is Fire?

Three elements of fire protection:

2. Fire detection

- It is recognizing that there is a fire.
- Fire detection devices can be
 - **smoke** activated,
 - **heat** activated, or
 - **flame** activated.

3. Fire containment and suppression

- It involves actually **responding** to the fire. Containment and suppression equipment is specific to fire classification.



How Dangerous Is Fire (Fire Classification)

- Responding to the fire based on its specific classification
 - **Class A:** Fire with combustible materials as its fuel source, such as wood, cloth, paper, rubber, and many plastics
 - **Class B:** Fire in flammable liquids, oils, greases, tars, oil-base paints, lacquers, and flammable gases
 - **Class C:** Fire that involves electrical equipment
 - **Class D:** Combustibles that involve metals



How Dangerous Is Fire (Fire Classification)

- Facilities must comply with standards to test fire-extinguishing methods annually to validate full functionality.
- The best-case scenario is that data centers and other critical locations are protected by an automatic fire-fighting system that spans multiple classes.
- In any emergency, human life always takes precedence. All personnel should know how to quickly and safely evacuate an area.



What About Disposal?

- What do servers, workstations, laptops, tablets, smartphones, firewalls, routers, copies, scanners, printers, memory cards, cameras, and flash drives have in common?
- They all store data that should be permanently removed before handing down, recycling, or discarding.



What About Disposal (Data Files)?

- The data can be apparent, hidden, temporary, cached, browser based, or metadata.
- **Apparent data files** are files that authorized users can view and access.
- **Hidden files** are files that the operating system by design does not display.
- **Temporary files** are created to hold information temporarily while a file is being created.
- **A web cache** is the temporary storage of web documents, such as HTML pages, images, and downloads.
- **A data cache** is the temporary storage of data that has recently been read and, in some cases, adjacent data areas that are likely to be accessed next.



What About Disposal (Data Files)?

- Browser-based data includes the following items:
 - **Browsing history**, which is the list of sites visited
 - **Download history**, which is the list of files downloaded
 - **Form history**, which includes the items entered into web page forms
 - **Search bar history**, which includes items entered into the search engines
 - **Cookies**, which store information about websites visited, such as site preferences and login status
- **Metadata** is details about a file that describes or identifies it, such as title, author name, subject, and keywords that identify the document's topic or contents.



Data Destruction Standard

- NIST Special Publication 800-88 defines data destruction as “the result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible to recover or prohibitively expensive.”



What About Disposal?

- Removing data from drives
 - Formatting a hard drive or deleting files does not mean that the data located on that drive cannot be retrieved
 - Two methods for permanently removing data from drives before their disposal:
 - **Disk wiping** (overwriting the hard drive with 0 and 1)
 - **Degaussing** (exposing the hard drive to high magnetic field)



What About Disposal?

- Disk wiping
 - The process will overwrite the master boot record (MBR), partition table, and every sector of the hard drive with the **numerals 0 and 1 several times**. Then the drive is formatted.
 - The **more times** the disk is overwritten and formatted, **the more secure the disk wipe is**.
 - Disk wiping **does not work** reliably on **solid-state drives**; USB thumb drives, compact flash, and MMC/SD cards.



What About Disposal?

- Degaussing
 - The process wherein a magnetic object, such as a computer tape, hard disk drive, or CRT monitor, is **exposed** to a **magnetic field** of greater, fluctuating intensity.
 - As applied to magnetic media, such as video, audio, computer tape, or hard drives, the movement of magnetic media through the degaussing field **realigns the particles**, **resetting the magnetic field** of the media to a **near-zero state**, erasing all the data written to the tape or hard drive.
 - In many instances, degaussing **resets** the media to a **like-new state** so that it can be reused and recycled.



What About Disposal?

- Destroying materials
 - The objective of physical destruction is to render the device and/or the media unreadable and unusable.
 - Devices and media can be crushed, shredded, or, in the case of hard drives, drilled in several locations perpendicular to the platters and penetrating clear through from top to bottom.
 - Cross-cut shredding technology, which reduces material to fine, confetti-like pieces, can be used on all media, ranging from paper to hard drives.



What About Disposal?

- Outsource the destruction process
 - Companies that offer destruction services often have specialized equipment and are cognizant of environmental and regulatory requirements.
 - The downside is that the organization is transferring responsibility for protecting information.
 - The media may be transported to off-site locations. The data is being handled by non-employees over whom the originating organization has no control.
- Selecting a destruction service is serious business, and thorough due diligence is in order.



Stop, Thief! (Statistics)

- According to the Federal Bureau of Investigation (FBI), on average, a laptop is stolen **every 53 seconds**
- **One in ten** individuals will have their laptop stolen at some point.
- The **recovery statistics** of stolen laptops is even worse, with only **3%** ever being recovered.
- This means **97% of laptops** stolen will **never be returned** to their rightful owners.



Stop, Thief! (Statistics)

- The **cost of lost** and stolen devices is **significant**. The most obvious loss is the device itself.
- The cost of the device pales in comparison to the **cost of detection, investigation, notification, after-the-fact response, and economic impact** of lost customer trust and confidence, especially if the device contained **legally protected information**.
- The Ponemon Institute “2013 Cost of Data Breach Study:
- Global Analysis” calculated the **average business cost** of a breach in the United States to be **\$188 per record** across all industries, **\$215 per record** for financial institutions, and **\$233 per record** for healthcare organizations.



Summary

- The physical perimeter of the company must be secured.
- Some internal rooms and offices must be identified as needing more security controls than others. These controls must be deployed.
- Environmental threats such as power loss or a fire must be taken into account and the proper hardware must be placed.
- A clean screen and desk policy is important to protect the confidentiality of company-owned data.
- It is important to permanently remove data before recycling or disposing of a device.



Thank You





الجامعة السعودية الإلكترونية
SAUDI ELECTRONIC UNIVERSITY
2011-1432

Bachelor of Science in
Information Technology
IT409
IT Security and Policies

Security Program and Policies

Principles and Practices

by Sari Stern Greene
Updated 02/2018



Objectives

- Recognize the importance of the CIA security model and describe the security objectives of confidentiality, integrity, and availability
- Discuss why organizations choose to adopt a security framework
- Recognize the values of NIST resources
- Understand the intent of ISO/IEC 27000-series of information security standards
- Outline the domains of an information security program



CIA

- The CIA Triad or CIA security model
 - Stands for Confidentiality, Integrity, and Availability
 - An attack against either or several of the elements of the CIA triad is an attack against the Information Security of the organization.
 - Protecting the CIA triad means protecting the assets of the company.



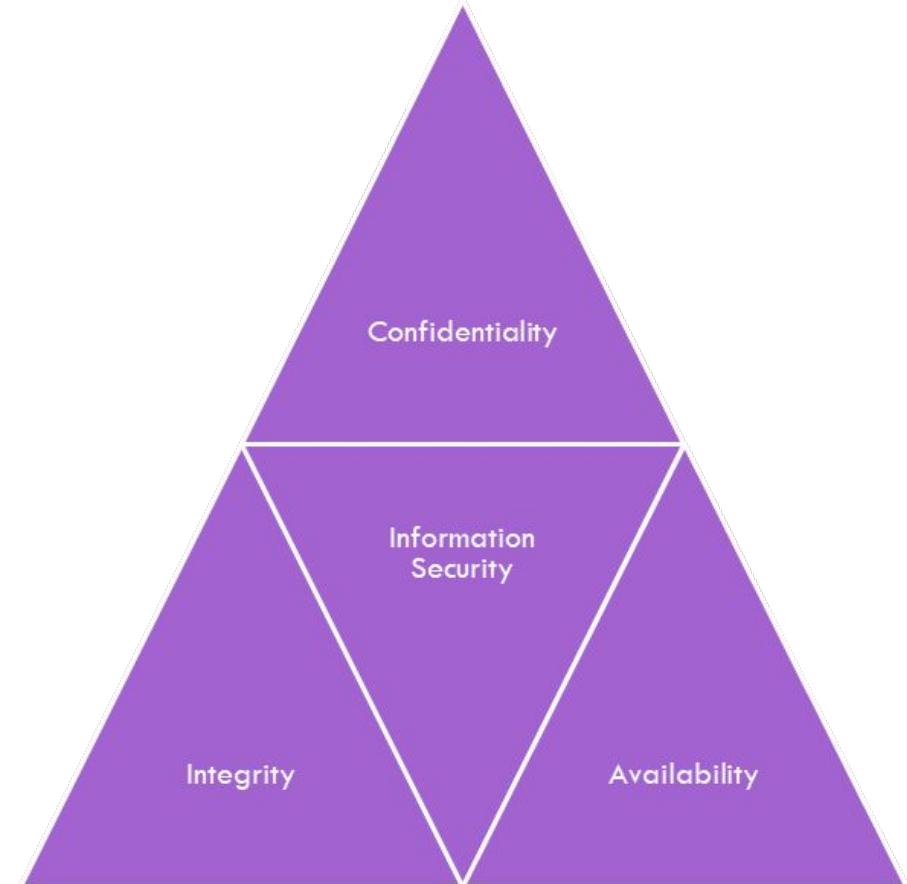
CIA

- The Federal Information Security Management Act (FISMA) defines the relationship between information security and the CIA triad as follows:
 - “information security” means protecting information and information systems in order to provide:
 - Integrity
 - Confidentiality and
 - Availability



CIA

- Organizations may consider all three components of the CIA triad equally important, in which case resources must be allocated proportionately.



What Is Confidentiality?

- Not all data owned by the company should be made available to the public
- Failing to protect data confidentiality can be disastrous for an organization:
 - Dissemination of Protected Health Information (PHI) between doctor and patient
 - Dissemination of Protected Financial Information (PFI) between bank and customer
 - Dissemination of business-critical information to rival company



What Is Confidentiality?

- It means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.



What Is Confidentiality? Cont.

- Only authorized users should gain access to information
- Information must be protected when it is used, shared, transmitted, and stored
- Information must be protected from unauthorized users both internally and externally
- Information must be protected whether it is in digital or paper format



What Is Confidentiality? Cont.

- The threats to confidentiality must be identified. They include:
 - Hackers and hacktivists
 - Shoulder surfing
 - Lack of shredding of paper documents
 - Malicious Code (Virus, worms, Trojans)
 - Unauthorized employee activity
 - Improper access control



What Is Confidentiality? Cont.

- The information security goal of confidentiality is to protect information from unauthorized access and misuse
- The best way to do this is to implement safeguards and processes that increase the work factor and the chance of being caught
- A spectrum of access controls and protections as well as ongoing monitoring, testing, and training



What Is Integrity? Cont.

- Protecting data, processes, or systems from intentional or accidental unauthorized modification
- Data integrity - A requirement that information and programs are changed only in a specified and authorized manner
- System integrity - A requirement that a system “performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system



What Is Integrity? Cont.

- A business that cannot trust the integrity of its data is a business that cannot operate
- An attack against data integrity can mean the end of an organization's capability to conduct business



What Is Integrity? Cont.

- Threats to data integrity include:
 - Human error
 - Hackers
 - Unauthorized user activity
 - Improper access control
 - Malicious code
 - Interception and alteration of data during transmission



What Is Integrity? Cont.

- Controls that can be deployed to protect data integrity include:
 - Access controls:
 - Encryption
 - Digital signatures
 - Process controls:
 - Code testing
 - Monitoring controls;
 - File integrity monitoring
 - Log analysis
 - Behavioral controls:
 - Separation of duties
 - Rotation of duties
 - End user security training



What Is Availability?

- Availability is the assurance that the data and systems are accessible when needed by authorized users
- The Service Level Agreement (SLA) is a type of agreement between a service provider and a customer that specifically addresses availability of services.
- What is the cost of the loss of data availability to the organization?
- A risk assessment should be conducted to more efficiently protect data availability.



What Is Availability? Cont.

- Threats to data availability include:
 - Natural disaster
 - Hardware failures
 - Programming errors
 - Human errors
 - Distributed Denial of Service attacks
 - Loss of power
 - Malicious code
 - Temporary or permanent loss of key personnel



What Is Availability? Cont.

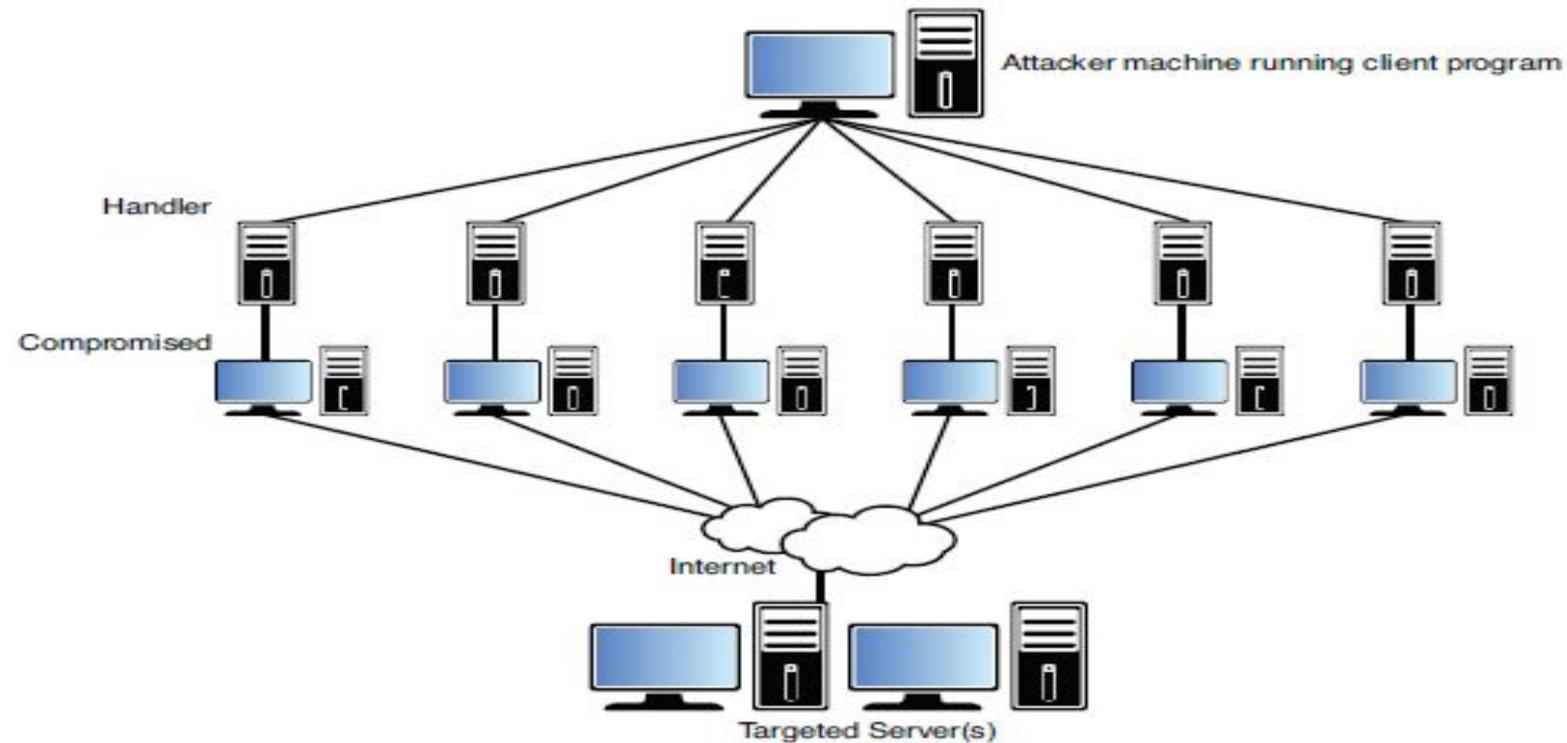


FIGURE 3.2 A conceptual diagram of a DDoS attack.



The Five A's of Information Security

- Supporting the CIA triad of information security are five key information security principles, commonly known as the Five A's:
 - Accountability
 - Assurance
 - Authentication
 - Authorization
 - Accounting



The Five A's of Information Security Cont.

▪Accountability:

- All actions should be traceable to the person who committed them.
- Logs should be kept, archived, and secured.
- Intrusion detection systems should be deployed.
- Computer forensic techniques can be used retroactively.
- Accountability should be focused on both internal and external actions.



The Five A's of Information Security Cont.

- **Assurance:**

- Security measures need to be designed and tested to ascertain that they are efficient and appropriate
- The knowledge that these measures are indeed efficient is known as assurance

- The activities related to assurance include:

- Auditing and monitoring
- Testing
- Reporting



The Five A's of Information Security Cont.

- **Authentication:**

- Authentication is the cornerstone of most network security models.
- It is the positive identification of the person or system seeking access to secured information and/or system.
- Examples of authentication models:
 - User ID and password combination
 - Tokens
 - Biometric devices



The Five A's of Information Security Cont.

▪ Authorization:

- Act of granting users or systems actual access to information resources.
- Note that the level of access may change based on the user's defined access level.
- Examples of access level include the following:
 - Read only
 - Read and write
 - Full



The Five A's of Information Security Cont.

• Accounting:

- Defined as the logging of access and usage of resources.
- Keeps track of who accesses what resource, when, and for how long.
- An example of use:
 - Internet café, where users are charged by the minute of use of the service.
 - CIA plus the Five A's are fundamental objectives and attributes of an information security program.



Who Is Responsible for CIA?

- Information owner:
 - An official with statutory or operational authority for specified information.
 - Has the responsibility for ensuring information is protected from creation through destruction.
- Information custodian:
 - Maintain the systems that store, process, and transmit the information.



Information Security Framework

- Security framework is a collective term given to guidance on topics related to:
 - information systems security
 - predominantly regarding the planning
 - Implementing
 - Managing and auditing of overall information security practices



Information Security Framework, Cont.

- Two of the most widely used frameworks are:
 - Information Technology and Security Framework by NIST
 - Information Security Management System by ISO



NIST Functions

- Founded in 1901
- Non regulatory federal agency
- Its mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve quality of life
- Published more than 300 information security-related documents including:
 - Federal Information Processing Standards.
 - Special Publication 800 series.
 - ITL bulletins.



NIST Functions

- NIST defines information security as:

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide CIA.



NIST Functions

- The mission of NIST's CSD is to improve information systems security as follows:
 - By raising awareness of IT risks, vulnerabilities, and protection requirements, particularly for new and emerging technologies.
 - By researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive federal systems.
 - By developing standards, metrics, tests, and validation programs
 - By developing guidance to increase secure IT planning, implementation, management, and operation.



ISO Functions

- A network of national standards institutes of 146 countries
- Nongovernmental organization that has developed more than 13,000 international **standards**.
- The ISO/IEC 27000 series represents information security standards published by ISO and Electro-technical Commission (IEC)



ISO 27002:2013 Code of Practice

- Comprehensive set of information security recommendations on **best practices** in information security.
- ISO 27002:2013 is organized in the following domains:
 - Information security policies (Section 5) – This domain focuses on information security policy requirements and the need to **align policy with organizational objectives**.
 - Organization of Information Security (Section 6) – This domain focuses on establishing and supporting a management structure to **implement and manage information security** within, across, and outside the organization.



ISO 27002:2013 Code of Practice

- Human Resources Security Management (Section 7) – This domain focuses on integrating security into the **employee lifecycle**, agreements, and training. Human nature is to be trusting.
- Asset Management (Section 8) – This domain focuses on developing **classification** schema, assigning classification levels, and maintaining accurate inventories of data and devices.



ISO 27002:2013 Code of Practice

- Access Control (Section 9) – This domain focuses on managing **authorized** access and preventing **unauthorized** access to information systems and extends to remote locations, home offices, and mobile access
- Cryptography (Section 10) – This domain was added in the 2013 update and it focuses on proper and effective use of **cryptography** to protect the CIA of information



ISO 27002:2013 Code of Practice

- Physical and Environmental Security (Section 11) – This domain focuses on **designing** and **maintaining** a **secure** physical environment to prevent unauthorized access, damage, and interference to business premises.
- Operations Security (Section 12) – This domain focuses on data centre operations, integrity of operations, **vulnerability management**, protection against data loss, and **evidence-based logging**.



ISO 27002:2013 Code of Practice

- Communications Security (Section 13) – This domain focuses on the protection of information in **transit**
- Information Systems Acquisition, Development, and Maintenance (Section 14) – This domain focuses on the **security requirements** of information systems, applications, and code from conception to destruction.



ISO 27002:2013 Code of Practice

- Supplier Relationships (Section 15) – This domain was added in the 2013 update. The domain focuses on service delivery, **third-party** security requirements, contractual obligations, and oversight.
- Information Security Incident Management (Section 16) – This domain focuses on a consistent and effective approach to the management of **information security incidents**, including detection, reporting, response, escalation, and forensic practices



ISO 27002:2013 Code of Practice

- Business Continuity (Section 17) – This domain focuses on availability and the secure provision essential services during a **disruption** of normal operating conditions.
- Compliance Management (Section 18) – This domain focuses on conformance with internal policy; local, national, and international criminal and civil **laws**; **regulatory** or contractual obligations; intellectual property rights (IPR); and copyrights



Summary

- The CIA triad is the blueprint of what assets needs to be protected to protect the organization.
- Protecting the organization's information security can seem vague and too conceptual. Protecting the confidentiality, integrity, and availability of the data is a concrete way of saying the same thing.
- Standards such as the ISO 27002 exist to help organizations better define appropriate ways to protect their information assets.



Thank You





الجامعة السعودية الإلكترونية
SAUDI ELECTRONIC UNIVERSITY
2011-1432

Bachelor of Science in
Information Technology
IT409
IT Security and Policies

Security Program and Policies

Principles and Practices

by Sari Stern Greene
Updated 02/2018



Week 14

Chapter 15: PCI Compliance for Merchants



Contents

1. Protecting Cardholder Data
2. PCI Compliance



Objectives

- Describe the PCI Data Security Standard framework
- Recognize merchant responsibilities
- Explain the 12 top-level requirements
- Understand the PCI DSS validation process
- Implement practices related to PCI compliance



Required Reading

1. Chapter 15 in Greene (2014)
2. "Best Practices for PCI 3.0 Compliance"



- Protecting Cardholder Data



Introduction

- Payment cards companies developed the Payment Card Industry Data Security Standard (PCI DSS) in order to protect cardholder information and to prevent fraud.
- Payment Cards examples: Visa, MasterCard, Discover, JCB International and American Express



Protecting Cardholder Data

- PCI DSS applies to all system components where account data is stored
 - Account data
 - Cardholder data plus sensitive authentication data
 - System components
 - Any network component, server, or application that is included in, or connected to, the cardholder data environment
 - Cardholder data environment
 - The people, processes, and technology that handle cardholder data or sensitive authentication data



Account Data Elements

TABLE 15.1 Account Data Elements

Cardholder Data Includes...	Sensitive Authentication Data Includes...
Primary account number (PAN)	Full magnetic stripe data or equivalent data on a chip
Cardholder name	CAV2/CVC2/CVV2/CID
Expiration date	PINs/PIB blocks
Service code	



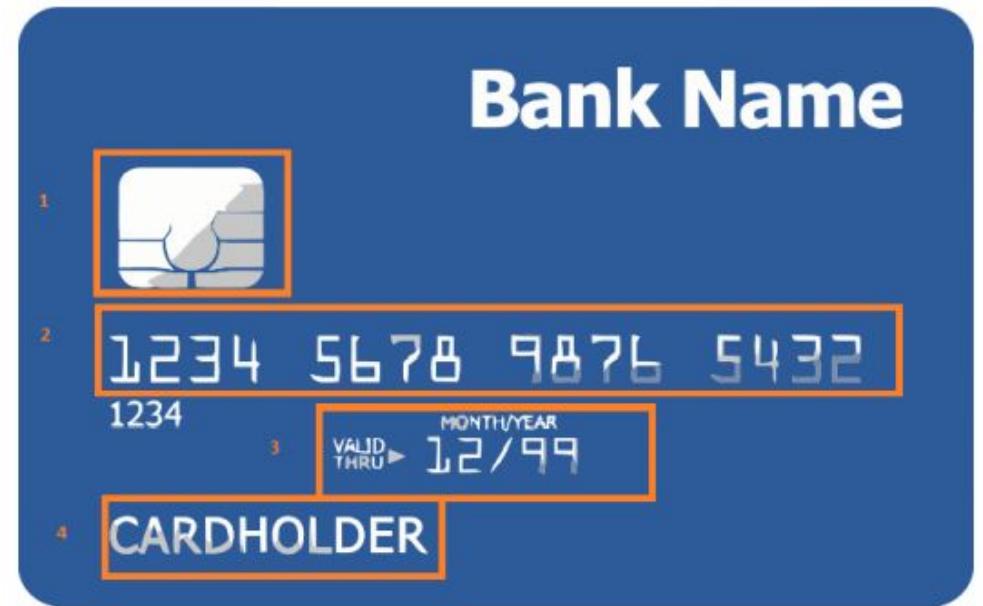
Protecting Cardholder Data Cont.

- Primary account number (PAN) must be stored in an unreadable (encrypted) format
- Sensitive authentication data may never be stored post-authorization, even if encrypted
- Utilizing a third party to store, process, and transmit cardholder data or manage system components does not relieve a covered entity of its PCI compliance obligation



Protecting Cardholder Data Cont.

- Figure shows the following elements located on the front of a credit card:
 1. Embedded microchip. contains the same information as the magnetic stripe.
 2. Primary account number (PAN).
 3. Expiration date.
 4. Cardholder name.



Protecting Cardholder Data Cont.

- Figure shows the following elements on the back of a credit card:
 1. Magnetic stripe (mag stripe)—The magnetic stripe contains encoded data required to authenticate, authorize, and process transactions.
 2. CAV2/CID/CVC2/CVV2—All refer to card security codes for the different payment brands.



What Is the PCI DSS Framework?

- The PCI DSS framework includes:
 1. Stipulations regarding storage, transmission, and processing of payment card data
 2. Six core principles
 3. Required technical and operational security controls
 4. Testing requirements
 5. Certification process



Business-as-Usual Approach

- Privacy and Security are part of ordinary, every day practice.
- Business-as-usual is defined as the inclusion of PCI controls as part of an overall risk-based security strategy that is managed and monitored by the organization.
- Compliance is an ongoing process
 - The organization must monitor required controls to ensure they are operating effectively.



PCI DSS Framework

- The **Six** PCI DSS core principles
 1. Build and maintain a secure network and systems
 2. Protect cardholder data
 3. Maintain a vulnerability management program
 4. Implement strong access control measures
 5. Regularly monitor and test networks
 6. Maintain an information security policy



PCI Top Level Requirements

- PCI Top Level Requirements are reflective of information security best practices.
 - Requirements are a short simple description of the required action
 - Sub-requirements contain extensive additional details and expectations



The 12 PCI Top Level Requirements

- The PCI DSS consists of six core principles, which are accompanied by the following 12 requirements:
 1. Install and maintain a firewall configuration to protect cardholder data.
 2. Do not use vendor-supplied defaults for system passwords and security parameters.
 3. Protect stored cardholder data.
 4. Encrypt transmission of cardholder data across open, public networks.
 5. Protect all systems against malware and regularly update antivirus software or programs.
 6. Develop and maintain secure systems and applications.



The 12 PCI Top Level Requirements

- The PCI DSS consists of six core principles, which are accompanied by the following 12 requirements: (continued)
 7. Restrict access to cardholder data by business need-to-know
 8. Identify and authenticate access to system components.
 9. Restrict physical access to cardholder data.
 10. Track and monitor all access to network resources and cardholder data.
 11. Regularly test security systems and processes.
 12. Maintain a policy that addresses information security for all personnel



PCI Top Level Requirements

First Core Principle: Build and maintain a secure network and systems

- Includes the following two requirements
 1. Install and maintain a firewall configuration to protect cardholder data
 2. Do not use vendor-supplied defaults for system passwords and security parameters



PCI Top Level Requirements

Second Core Principle: Protect Cardholder Data

- Includes the following two requirements
 - 3. Protect stored card data
 - 4. Encrypt transmission of cardholder data across open, public networks



PCI Top Level Requirements

Third Core Principle: Maintain a Vulnerability Management Program

- Includes the following two requirements
 - 5. Protect all systems against malware and regularly update antivirus software or programs
 - 6. Develop and maintain secure systems and architecture



PCI Top Level Requirements

Fourth Core Principle: Implement Strong Access Control Measures

- Includes the following three requirements
7. Restrict access to cardholder data by business need-to-know
 8. Identify and authenticate access to system components
 9. Restrict physical access to cardholder data



PCI Top Level Requirements

Fifth Core Principle: Regulatory Monitor and Test Networks

- Includes the following two requirements
 - 10. Track and monitor all access to network resources and cardholder data
 - 11. Regularly test security systems and processes



PCI Top Level Requirements

Sixth Core Principle: Maintain an Information Security Policy

- Includes the final requirement
12. Maintain a policy that addresses information security for all personnel



- PCI Compliance



PCI Compliance

- PCI compliance is **not** a government regulation or law
- It's mandated by the payment card brands to accept card payments and/or be part of the payment system
- Merchants are required to comply with PCI DSS
 - A merchant is defined as any entity that accepts American Express, Discover, JCB, MasterCard, or Visa payment cards as payment for goods and/or services (including donations)
 - Effectively, any company, organization, or individual that accepts card payments is a merchant



.PCI Compliance Cont

- PCI compliance validation is composed of **four levels**, based on the number of transactions processed per year and whether those transactions are performed from a physical location or over the Internet
 - Level 1
 - Processes **more than 6 million** Visa payment card transactions annually
 - Level 2
 - Processing **1million to 6million** Visa transactions per year.
 - Level 3
 - Any merchant processing **20,000 to 1,000,000** Visa e-commerce transactions per year
 - Level 4
 - Any merchant processing **fewer than 20,000** Visa e-commerce transactions per year, and all other merchants—regardless of acceptance channel—processing up to **1million** Visa transactions per year



What Is a Data Security Compliance Assessment

- An annual onsite evaluation of compliance with the PCI DSS conducted by either a Qualified Security Assessor (QSA) or an Internal Security Assessor (ISA)
 - **Qualified Security Assessors (QSAs)** are organizations that have been qualified by the PCI Council to have their employees assess compliance to the PCI DSS standard. QSAs are employees of these organizations who have been certified by the council to validate an entity's adherence to the PCI DSS.
 - **Internal Security Assessors (ISAs)** are sponsor companies that have been qualified by the council. The PCI SSC ISA Program consists of internal security audit professionals of sponsor organizations who are qualified through training from the council to improve their organization's understanding of the PCI DSS.



What Is a Data Security Compliance Assessment

- **Assessment process** begins with documenting the PCI DSS cardholder environment and confirming the scope of the assessment
- QSA/ISA will conduct an initial assessment (GAP assessment) identify areas of noncompliance and provide remediation recommendations
- Post-remediation, the QSA/ISA will conduct the assessment.



What Is a Data Security Compliance Assessment

- In order to complete the process, the following must be submitted to either the acquiring financial institution or payment card brand:
 - ROC completed by a QSA or ISA
 - Evidence of passing vulnerability scans by an ASV
 - Completion of the Attestation of Compliance by the assessed entity and the QSA
 - Supporting documentation



Compliance Assessment

- Compliance Assessment
 - On-Site evaluation of compliance with PCI-DSS
- Assessment Methodology
 - Observe system settings
 - Observe processes and actions that use cardholder data
 - Review documentations
 - Interview system users
 - Run test data through system (Sampling)
- Create Report on Compliance (ROC) document



Report on Compliance

- ROC standard template includes the following
 - Section 1: Executive Summary
 - Section 2: Description of Scope of Work and Approach Taken
 - Section 3: Details About Reviewed Environment
 - Section 4: Contact Information and Report Date
 - Section 5: Quarterly Scan Results
 - Section 6: Findings and Observations
 - Compensating Controls Worksheets (if Applicable)



?What Is the SAQ

- SAQ: Self Assessment Questionnaire
 - Several versions for different types of merchants
- A validation tool for merchants that are not required to submit to an onsite data security assessment
- Has two parts
 - Controls questionnaire
 - Self-certified attestation



SAQ categories

- There are five SAQ categories and the number of questions vary because the questionnaires are designed to be reflective of the specific payment card channel and the anticipated scope of the cardholder environment
 1. SAQ A (13 questions) is applicable to merchants who retain only paper reports or receipts with cardholder data. This would never apply to face-to-face merchants.
 2. SAQ P2PE (18 questions) is applicable to merchants who process cardholder data only via payment terminals included in a validated and PCI SSC–listed Point-to-Point Encryption (P2PE) solution. This would never apply to e-commerce merchants. This category was added in June 2012.



SAQ categories

3. SAQ B (29 questions) is applicable to merchants who process cardholder data only via imprint machines or standalone, dial-out terminals. This would never apply to e-commerce merchants.
4. SAQ C-VT (51 questions) is applicable to merchants who process cardholder data only via isolated virtual terminals on personal computers connected to the Internet. This would never apply to e-commerce merchants.
5. SAQ C (80 questions) is applicable to merchants whose payment application systems are connected to the Internet either because the payment application system is on a personal computer that is connected to the Internet.



SAQ categories

- SAQ D (288 questions) is applicable to all other merchants not included in descriptions for SAQ types A through C as well as all service providers defined by a payment brand as eligible to complete an SAQ.



Completing the SAQ

- In order to achieve compliance in question, the response to each question must either be “yes” or an explanation of a compensating control.
- If an entity cannot provide affirmative responses, it is still required to submit an SAQ
- To complete the validation process, the entity submits the SAQ and an accompanying Attestation of Compliance stating that it is or is not compliant with the PCI DSS.
- If the attestation indicates noncompliance, a target date for compliance along with an action plan needs to be provided.



?Are There Penalties for Noncompliance

- Three type of fines
 - 1. PCI noncompliance
 - discretionary and can vary greatly, depending on the circumstances
 - 2. Account Data Compromise Recovery (ADCR) for compromised domestic-issued cards
 - 3. Data Compromise Recovery Solution (DCRS) for compromised international-issued cards
- Fine paid by issuing bank. May be passed on to merchant.



Summary

- The Payment Card Industry Data Security Standard, known as PCI DSS, applies to all entities involved in the payment card channel, including merchants, processors, financial institutions, and service providers, as well as all other entities that store, process, or transmit cardholder data and/or sensitive authentication data
- The PCI DSS framework includes six core principles and 12 categories of required technical and operational security controls, testing requirements, and a validation and certification process
- Compliance with PCI DSS is a payment card channel contractual obligation. It is not a government regulation or law



Thank You





الجامعة السعودية الإلكترونية
SAUDI ELECTRONIC UNIVERSITY
2011-1432

Bachelor of Science in
Information Technology
IT409
IT Security and Policies

Security Program and Policies

Principles and Practices

by Sari Stern Greene
Updated 02/2018



Objectives

- Define a disaster
- Appreciate the importance of **emergency preparedness**
- Analyze threats, risks, and **business impact assessments**
- Explain the components of a **business continuity plan** and program
- Develop policies related to business continuity management



Objectives

- The objective of the Business Continuity Management domain is to ensure the continued operation and secure provision of essential services during a disruption of normal operating conditions.
- To support this objective, **threat scenarios** are evaluated, essential services and processes are identified, and response, contingency, and recovery and resumption strategies, plans, and procedures are developed, tested, and maintained.
- **Business continuity** is a component of organization risk management.



Emergency Preparedness

■ Disaster

- Any event that results in damage or destruction, **loss of life**, or drastic change to the environment
- A disruption of normal business functions where the expected time for returning to normalcy would **seriously** impact the organization's capability to maintain operations, including customer commitments and regulatory compliance
- The cause can be environmental, operational, accidental, or willful



Emergency Preparedness Continue....

- Environmental events:

- include severe weather, earthquakes, tornados, fire, flood, air contaminants, and public health emergencies.

- Operational issues:

- include failures or misconfiguration of equipment, disruption of communication systems, unavailability of third-party systems or personnel, and degradation of power.



Emergency Preparedness Continue....

- Accidents:

- include nuclear, biological, or hazardous chemical exposure, explosions, and user or operator error.

- Willful damage:

- includes terrorism, sabotage, civil disturbances, war, workplace violence, and cybercrime.

The U.S. Department of Homeland Security (DHS) has identified the Impact of **15 disaster scenarios** that could take the country **days** (explosives) to **weeks** (food contamination) to **months** (pandemic, major hurricane) to **years** (nuclear detonation, major earthquake) to potentially recover from.



Emergency Preparedness cont.

- Resilient organization
 - Has the capability to **quickly** adapt and recover from known or unknown change to the environment
 - Business disruption has an economic and societal ripple effect
- **Emergency preparedness** is a civic duty and regulatory requirement



Business Continuity Risk Management

- Continuity planning
 - The business practice of ensuring the execution of **essential functions**
 - Component of organizational risk management
 - Risk management for continuity of operations requires the organizations to
 - Identify the **threats** that can disrupt operations
 - Determine the **risk**
 - **Assess the impact** on the company



Business Continuity Risk Management cont.

- Business continuity threat assessment
 - Identify viable threats and predict the likelihood of occurrence
- Business continuity risk assessment
 - Evaluates the sufficiency of controls to prevent a threat from occurring or to minimize its impact



Business continuity threat assessment

- A business continuity threat can best be defined as a **potential danger** to the organization.
- Threats can be business specific, local, regional, national, or even global.
- The objective of a business continuity threat assessment is to **identify viable threats** and **predict the likelihood of occurrence**.



Business continuity threat assessment

- Threat modeling takes into account **historical** and **predictive** geographic, technological, physical, environmental, third-party, and industry factors such as the following:
- What type of disasters have occurred in the community or at this location?
- What can happen due to the geographic location?



Business continuity threat assessment

- What could cause processes or information systems to fail?
- What threats are related to service provider dependency?
- What disasters could result from the design or construction of the facility or campus?
- What hazards are particular to the industry sector?



What Is a Business Continuity Risk Assessment?

- The business continuity threat assessment identifies the most likely and significant business continuity related threats to the organization.



What Is a Business Continuity Risk Assessment?

- The **business continuity risk assessment** evaluates the sufficiency of controls to prevent a threat from occurring or to minimize its impact.
- The outcome is the **residual** risk associated with each threat.
- The residual risk level provides management with an accurate portrayal of what happens if the threat is exercised under current conditions.



What Is a Business Continuity Risk Assessment?

- In a best-case scenario, the residual risk is within organizational tolerance.
- If the residual risk is **not within tolerance**, the organization must decide to **take action to lower the risk level**, approve the risk, or share the risk.
- Lowering the risk level requires the organization to implement **additional controls and safeguards** and/or to modify existing ones.
- Risk sharing is when the **risk** (and consequences) are distributed among two or more parties. Examples are outsourcing and insurance.



What Is a Business Impact Assessment?

- **Business Impact Analysis**

- Identify essential services/processes and recovery timeframes
- It is a multistep collaborative activity that involves business process owners, stakeholders, and corporate officers



Business Impact Analysis cont.

A business impact analysis is a multistep collaborative activity that should include business process owners, stakeholders, and corporate officers:

Step 1: Identify essential business **services** and processes.

Step 1A: Determine the maximum tolerable downtime for each service.

Step 2: Identify supporting infrastructure, information systems, and dependencies.

Step 2A: Determine recovery time objectives and recovery point objectives



Business Impact Analysis cont.

Step 3: Compare to current recovery capability. Step 3A: Document the gap between desired and current capabilities.

Step 4: Have stakeholders review the report for accuracy.

Step 5: Present the BIA to management for approval.



A BIA incorporates three metrics

- The maximum tolerable downtime (MTD) is the total length of time an essential business function can be unavailable without causing significant harm to the business.
- The recovery time objective (RTO) is the maximum amount of time a system resource can be unavailable before there is an unacceptable impact on other system resources or business processes.
- The recovery point objective (RPO) represents the point in time, prior to a disruption or system outage, that data can be recovered (in other words, the acceptable data loss).



Business Continuity Plan

- The objective is to ensure the organization has the capability to respond and recover from a **disaster**
- Component of Business Continuity Plan:
- **Response plans** (focus on the initial and near-term response and include such elements as authority, plan activation, notification, communication, evacuation, relocation, coordination with public authorities, and security)



Business Continuity Plan comp.

- **Contingency plans** (focus on immediate, near-term, and short-term alternate workforce and business processes)
- **Recovery plans** (focus on the immediate, near-term, and short-term recovery of information systems, infrastructure, and facilities)
- **Resumption plans** (guide the organization back to normalcy)



Business Continuity Plan cont.

- Business continuity management involves the entire organization
 - Board of Directors provides oversight and guidance, authorizes the related policy, and is legally accountable for the actions of the organization
 - Executive management provides leadership
 - Business Continuity Team (BCT) has the authority to make decisions related to disaster preparation, response, and recovery



Business Continuity Plan cont.

- **Roles and Responsibilities:** Business continuity responsibilities can be categorized as governance, operational, and tactical.
 - **Governance:** It is a continuing process in which diverse objectives, competing interests, and a range of ideas are evaluated and ultimately binding decisions are made and supported.
 - **Operational Management:** When disaster strikes, quick mobilization is essential to mitigate damages. It is imperative that there be designated leadership with the authority to act quickly.
 - **Tactical Activities:** Tactical responsibilities are distributed throughout an enterprise. Depending on the size of the organization, some of these responsibilities may be consolidated.



Disaster Response Plans

- Addresses what should be done **immediately** following a significant incident
 - Defines who has the authority to declare a disaster
 - Defines who has the authority to contact external entities
 - Defines evacuation procedures
 - Defines emergency communication & notification procedures
- Upon declaration of a disaster, all BCT members should report to a designated command and control center
- Occupant emergency Plan (OEP)
 - Describes evacuation and shelter-in-place procedures in the event of a threat or incident to the health and safety of personnel



Disaster Response Plans cont.

- Relocation strategies

- Hot site

- Fully operational location with redundant equipment.
 - The data has been streamed to the site on a real-time basis or close to real time

- Warm site

- Configured to support operations including communications capabilities, peripheral devices, power, and HVAC.
 - Spare computers may be located there that then would need to be configured in the event of a disaster
 - Data must be restored



Disaster Response Plans cont.

▪ Relocation strategies

- Cold site
 - Available alternative location
 - Equipped with power, HVAC, and secure access
- Mobile site
 - Self-contained unit
 - Equipped with the required hardware, software, and peripherals
 - Data needs to be restored



Operational Contingency Plans

- Addresses how an organization's essential business processes will be delivered during the recovery process
- Developed at the departmental level
- Responsibility of the business process owner
- The documentation should follow the same form as the SOPs



The Disaster Recovery Phase

- Recovery strategies
 - The path to bringing the company back to a normal business environment
 - A plan should be in place that breaks down each category of the overall recovery effort to simplify the daunting recovery process:
 - Mainframe
 - Network
 - Communications
 - Infrastructure
 - Facilities



The Disaster Recovery Phase Cont.

- **Mainframe recovery** is specific to the restoration a mainframe computer (or equivalent capability) and corresponding data processing.
- **Network recovery** is specific to information systems (servers, workstations, mobile devices, applications, data stores, and supporting utilities) and includes the restoration of functionality and data.



The Disaster Recovery Phase Cont.

- **Communications recovery** encompasses internal and external transmission systems, including local area network (LAN), wide area network (WAN), data circuits (T1, T3, MPLS), and Internet connectivity.
- **Infrastructure recovery** encompasses those systems providing a general operating environment, including environmental and physical controls.
- **Facilities recovery** addresses the need to rebuild, renovate, or relocate the physical plant.



The Disaster Recovery Phase Cont.

- Recovery procedures

- All procedures should be designed, tested, documented, and approved prior to when the disaster strikes
- Procedures should be written as if the person who will be following them is not intimately familiar with the information system or component
- Procedures should explain what needs to be done, when, where, and how
- The key is to respond fast using predefined steps
- Recovery procedures should be **reviewed annually**



The Resumption Phase

The objective is to transition to normal operations

- Two major activities
 - Validation
 - Verifying recovered systems are operating correctly
 - Deactivation
 - The official notification that the organization is no longer operating in emergency or disaster mode



Plan Testing and Maintenance

- Proactive testing of the plan is essential
- Until tested, the plan is theoretical at best
- The tests should prove that the procedures and the plan are:
 - Relevant
 - Operable under adverse conditions
 - Accurate
- Tests are used to discover **errors** and **inadequacies**



Plan Testing and Maintenance Cont.

- Three standard testing methodologies
 - Tabletop exercise (focuses on participant readiness)
 - Structured review
 - Simulation
 - Functional exercises (allow personnel to validate plans, procedures, resource availability, and participant readiness.)
 - Full-scale testing (specific scenario)
- Business continuity plan audit
 - Evaluation of how the business continuity program in its entirety is being managed
 - Auditors must be independent



Business continuity plan audit Cont.

Auditors will look at the quality and effectiveness of the organization's BCP process, and determine whether the testing program is sufficient. At a minimum, you can anticipate they will ask the following questions:

- Is there a **written** business continuity policy and plan?
- Has the business continuity policy and plan been **approved** by the Board of Directors?



Business continuity plan audit Cont.

- How often is it reviewed and/or reauthorized?
- How often is a BIA conducted? By whom?
 - What training has the user community had?
- Are the results documented?
- If third parties are involved, what is the process for testing/verifying their procedures?
- Who is responsible for maintaining the plan?



Plan Maintenance

- Business environments are dynamic: The plan should be reviewed and edited regularly to match the changes that occur in the company and/or the industry in which the company is involved
- The plan cannot be reviewed without the risk assessment being reviewed as well
- Responsibility for maintaining the plan should be assigned to a specific role such as the ISO



Summary

- A **disaster** can strike at any time. The organization must be prepared to respond to continue to provide **services/products** to its clients.
- It is the responsibility of executive management to insure that threats are evaluated, impact to business processes recognized, and resources allocated.
- This requires the creation and maintenance of an audited **business continuity plan** and of a set of ancillary procedures.



Thank You





الجامعة السعودية الإلكترونية
SAUDI ELECTRONIC UNIVERSITY
2011-1432

Bachelor of Science in
Information Technology
IT409
IT Security and Policies

Security Program and Policies

Principles and Practices

by Sari Stern Greene
Updated 02/2018



Week 5

Chapter 5: Asset Management



Contents

1. Information Assets and Systems
2. Information Classification
3. Labeling and Handling Standards
4. Information Systems Inventory



Objectives

- Assign information ownership responsibilities
- Develop and use information classification guidelines
- Understand information handling and labeling procedures
- Identify and inventory information systems
- Create and implement asset classification policies



Required Reading

1. Chapter 15 in Greene (2014)



- Information Assets and Systems



Information Assets and Systems

- What is an information asset?
 - A definable piece of information, stored in any manner, and recognized as having value to the organization
 - It includes raw, mined, developed, and purchased data
 - The information is used by the company (regardless of size) to fulfill its mission or goal
 - Could be any information, such as customer and employees data, research and proprietary data, intellectual property data, and operational plans and procedures that have value to the company



Information Assets and Systems cont.

- Information Systems
 - Provide a way and a place to process, store, transmit, and communicate the information
 - Usually a combination of both hardware and software assets
 - Can be off-the-shelf or customized systems
- If compromised the consequences could include embarrassment, legal liability, financial ruin, and even loss of life



Example of Information Assets and Systems

- Data stores or warehouses of information about customers, personnel, production, sales, marketing, or finances.
- Intellectual property (IP) such as drawings, patents, music scores or other publication that have commercial value
- Operational plans and procedures that have value to the company
- Research documentation
- Strategic and operational plans and procedures that define the organization



Information Assets and Systems cont.

- Information Ownership
 - ISO stands for information security officer
 - The ISO is accountable for the protection of the organization. Compare this with:
 - The information owner is responsible for the information he owns
 - The information custodian is responsible for implementing the actual controls that protect the information assets
 - The ISO is the central repository of security information



Role of Data Owner

- Defining the asset
 - Assigning value to the asset
 - Defining the level of protection required
 - Deciding who should have access to the asset
 - Delegating day-to-day security and operational tasks
 - Ongoing governance
- not the one who will be tasked with implementing security controls



Role of Information Security Officer

- Accountable for the protection of the information asset.
- Managing the day-to-day controls
- Provide direction and guidance as to the appropriate controls and to ensure that controls are applied consistently throughout the organization
- ISO central repository of security information
- Publishes the classification criteria, maintains the information systems inventories, and implements broad strategic and tactical security initiatives



Information Ownership Policy Statement

- All information assets and systems must have an assigned owner.
- The Office of Information Security will maintain an inventory of information ownership.
- Owners are required to classify information and information systems in accordance with the organizational classification guidelines.
- Owners are responsible for determining the required level of protection.
- Owners must authorize internal information and information system access rights and permissions. Access rights and permissions must be reviewed and approved annually.
- Owners must authorize third-party access to information or information systems. This includes information provided to a third party.
- Implementation and maintenance of controls is the responsibility of the Office of Information Security; however, accountability will remain with the owner of the asset.



- Information Classification



Information Classification

- Objective of an information classification system is to differentiate data types.
- Definitions:
 - Information Classification
 - Information classification is the organization of information assets according to their sensitivity to disclosure
 - Classification Systems
 - Classification systems are labels that we assign to identify the sensitivity levels



Information Classification Lifecycle Process

- Assignment of classification ends with declassification. The information owner is responsible for managing this process.
 - Document the information asset and the supporting information systems.
 - Assign a classification level.
 - Apply the appropriate labeling.
 - Document “special” handling procedures (if different from organizational standards).
 - Conduct periodic classification reviews.
 - Declassify information when (and if) appropriate.



Classification Systems

- FIPS-99
 - Sensitivity of the data to be protected
- Government and Military
 - Based on Executive order of who is handling the data
- Commercial
 - As per the organization's hierarchy, decided by the information owner



Information Classification Cont.

- Federal Information Processing Standard 199 (FIPS-199) requires information owners to classify information and information systems based on CIA criteria as:
 - Low potential impact
 - Moderate potential impact
 - High potential impact



Information Classification Cont.

- (FIPS-199) classification
 - Low potential impact
 - the loss of CIA could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals
 - Moderate potential impact
 - the loss of CIA could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
 - High potential impact
 - the loss of CIA could be expected to have a **severe** or catastrophic adverse effect on organizational operations, organizational assets, or individuals
- SC of information type = {(confidentiality, impact), (integrity, impact), (availability, impact)},



Examples of FIPS-199 classification

- An organization managing public information on its web server determines that there is no potential impact from a loss of confidentiality (that is, confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability
- The resulting SC of this information type is expressed as follows:
- Security Category (SC) public information = {(confidentiality, n/a), (integrity, moderate), (availability, moderate)}



Information Classification Cont.

- Government & Military Classification Systems
 - Top Secret (TS)
 - Secret (S)
 - Confidential (C)
 - Unclassified (U)
 - Sensitive But Unclassified (SBU)



Information Classification Cont.

- Top Secret (TS)
 - Applied to “any information or material the unauthorized disclosure of which reasonably could be expected to cause an **exceptionally grave damage** to the national security”
- Secret (S)
 - Applied to “any information or material the unauthorized disclosure of which reasonably could be expected to cause **serious damage** to the national security”



Information Classification Cont.

- Confidential (C)
 - Applied to “any information or material the unauthorized disclosure of which reasonably could be expected to cause **damage** to the national security”
- Unclassified (U)
 - Applied to “any information that can generally be distributed to the public without any threat to national interest”



Information Classification Cont.

- Sensitive But Unclassified (SBU)
 - Applied to “any information of which the loss, misuse or unauthorized access to, or modification of might adversely affect U.S. National Interests, the conduct of the Department of Defense (DoD) programs or the privacy of DoD personnel”



Information Classification Cont.

- Commercial classification systems:
 - No standard: Each company can choose its own system that matches its culture and needs
 - Usually less complex than the government system
 - The more regulated a company, the more complex the classification system it adopts



Information Classification Cont.

- Commercial classification systems
 - Most systems revolve around these four classification levels:
 - Protected
 - Confidential
 - Internal Use
 - Public



Information Classification Cont.

- Commercial classification systems
 - Protected
 - Data protected by law, regulation, memorandum of agreement, contractual obligation, or management discretion
 - Examples: Social Security numbers, personal health information, financial information
 - Confidential
 - Data essential to the mission of an organization
 - Only available to a small circle of authorized individuals
 - Disclosure would cause significant financial loss, reputation loss and/or legal liability



Information Classification Cont.

- Commercial classification systems

- Internal Use:

- Data necessary for conducting ordinary company business
 - Loss, disclosure, and corruption **may** impair the business and lead to business, financial, or legal **loss**

- Public:

- Information that does not require protection
 - Information that is specifically intended for the public



Information Classification Policy

- Synopsis:

- An information classification system will be used to categorize information and information systems. The classification will be used to design and communicate baseline security controls.

- Policy Statement:

- The company will use a four-tiered data classification schema consisting of protected, confidential, restricted, and public.
- The company will publish definitions for each classification.
- The criteria for each level will be maintained by and available from the Office of Information Security.
- All information will be associated with one of the four data classifications. It is the responsibility of information owners to classify data.



Information Classification Policy

- Policy Statement: (continued..)

- Information systems containing information from multiple classification levels will be secured in accordance with the requirements of the highest classification level.
- Data classification will remain in force regardless of the location or state of the data at any given time. This includes backup and archive mediums and locations.
- The classification system will allow that classifications of information assets may change over time.
- Each classification will have handling and protection rules. The Office of Information Security is responsible for the development and enforcement of the handling and protection rules.



Reclassification/Declassification

- The need to protect information may **change**
- With that change, the **label** assigned to that information may change as well
- The process of **downgrading** sensitivity levels is called **declassification**
- The process of **upgrading** sensitivity levels is called **reclassification**



- Labeling and Handling Standards



Labeling and Handling Standards

- Information labeling:
 - **Labeling** is the vehicle for communicating the assigned classification to information custodians and users
 - Labels must be clear and self-explanatory
 - In electronic form, the label should be made part of the filename
 - In printed form, the label should be clearly visible on the outside and in the header and/or footer



Labeling and Handling Standards

- Information handling:
 - Information must be handled in accordance with its **classification**.
 - **Handling standards** inform custodians and users how to treat the information they use and the systems they interact with.
 - Handling standards generally include storage, transmission, communication, access, retention, destruction, and disposal, and may extend to incident management and breach notification



- Information Systems Inventory



Information Systems Inventory

- Many organizations don't have an up-to-date inventory
- Creating a comprehensive inventory of information systems is a major task
- Both **hardware** and **software** assets should be inventoried
- Each asset should have a **unique identifier** and a description
- Company assets should be accounted for at all times
- An asset management **procedure** should exist for **moving** and **destroying** assets



Information Systems Inventory cont.

- **Hardware assets** include (but are not limited to): visible and tangible pieces of equipment and media, such as:
 - Computer equipment
 - Printers
 - Communication and network equipment
 - Storage media
 - Infrastructure equipment



Information Systems Inventory cont.

- **Software assets** include (but are not limited to): programs or code that provide the interface between the hardware, the users, and the data. Generally fall into three categories
 - Operating system software
 - Productivity software
 - Application software



Summary

- A company cannot defend its information assets unless it knows what it is and where it is. Furthermore, the company must also identify how **critical** these **assets** are to the **business process**.
- FISMA requires federal agencies to classify their information and information systems as **low**, **moderate**, or **high** security based on criteria identified in **FIPS-199**.
- Companies need an **inventory** of their assets and a **classification system** for those assets.



Thank You





الجامعة السعودية الإلكترونية
SAUDI ELECTRONIC UNIVERSITY
2011-1432

Bachelor of Science in
Information Technology
IT409
IT Security and Policies

Security Program and Policies

Principles and Practices

by Sari Stern Greene
Updated 02/2018



*Chapter 13: Regulatory Compliance for
Financial Institutions*



Objectives

- Explain financial institution information security regulatory compliance requirements
- Understand the responsibilities SAMA- and CMA
- To study the cyber security framework of SAMA and its components



Introduction

- A financial institution's most significant asset is not money: It's information about money, transactions and customers
- Protection of those information assets is necessary to establish the required trust for the institution to conduct business
- Institutions have a responsibility to protect their client's information and privacy from harm such as fraud and ID theft



Who regulates banking and financial services in Saudi Arabia?

- The Kingdom of Saudi Arabia has two regulators with responsibility for the authorization and supervision of banks, insurance companies and other financial institutions
 - The Saudi Central Bank (SAMA), formerly known as Saudi Arabian Monetary Agency
 - Capital Market Authority (CMA)



Responsibilities of SAMA

- The SAMA regulates the following entities:
 - Conventional banks (deposit takers)
 - Insurance companies that engage in any insurance and re-insurance activities, including general insurance, health insurance and protection and savings insurance
 - Finance companies that engage in real estate finance, production asset finance, small and medium enterprise finance, finance lease, credit card finance, consumer finance, micro finance and any other finance activity approved by the SAMA



SAMA Act continued

- Given that the above entities are regulated by the SAMA, no banking business, insurance or re-insurance activity or finance activity may be engaged in Saudi Arabia without obtaining a **license** from the SAMA.
- It is strictly prohibited to conduct any of the activities listed above without obtaining a license from the SAMA.



CMA

- The CMA regulates financial institutions that conduct **securities** business (“Authorized Persons”).
- Such Authorized Persons include investment banks, asset managers, brokers and financial advisers.



CMA ..contd.

- The CMA is entrusted with the following duties:
 - Regulate and develop the capital market and promote appropriate standards and techniques for all sections and entities involved in Securities Trade Operations.
 - Protect investors and the public from unfair and unsound practices involving fraud, deceit, cheating, manipulation, and inside information trading.
 - Maintain fairness, efficiency, and transparency in transactions of securities.
 - Develop appropriate measures to reduce risks pertaining to transactions of securities.
 - Develop, regulate, and monitor the issuance of securities and under-trading transactions.
 - Regulate and monitor the activities of entities working under CMA.
 - Regulate and monitor full disclosure of information related to securities and issuers.

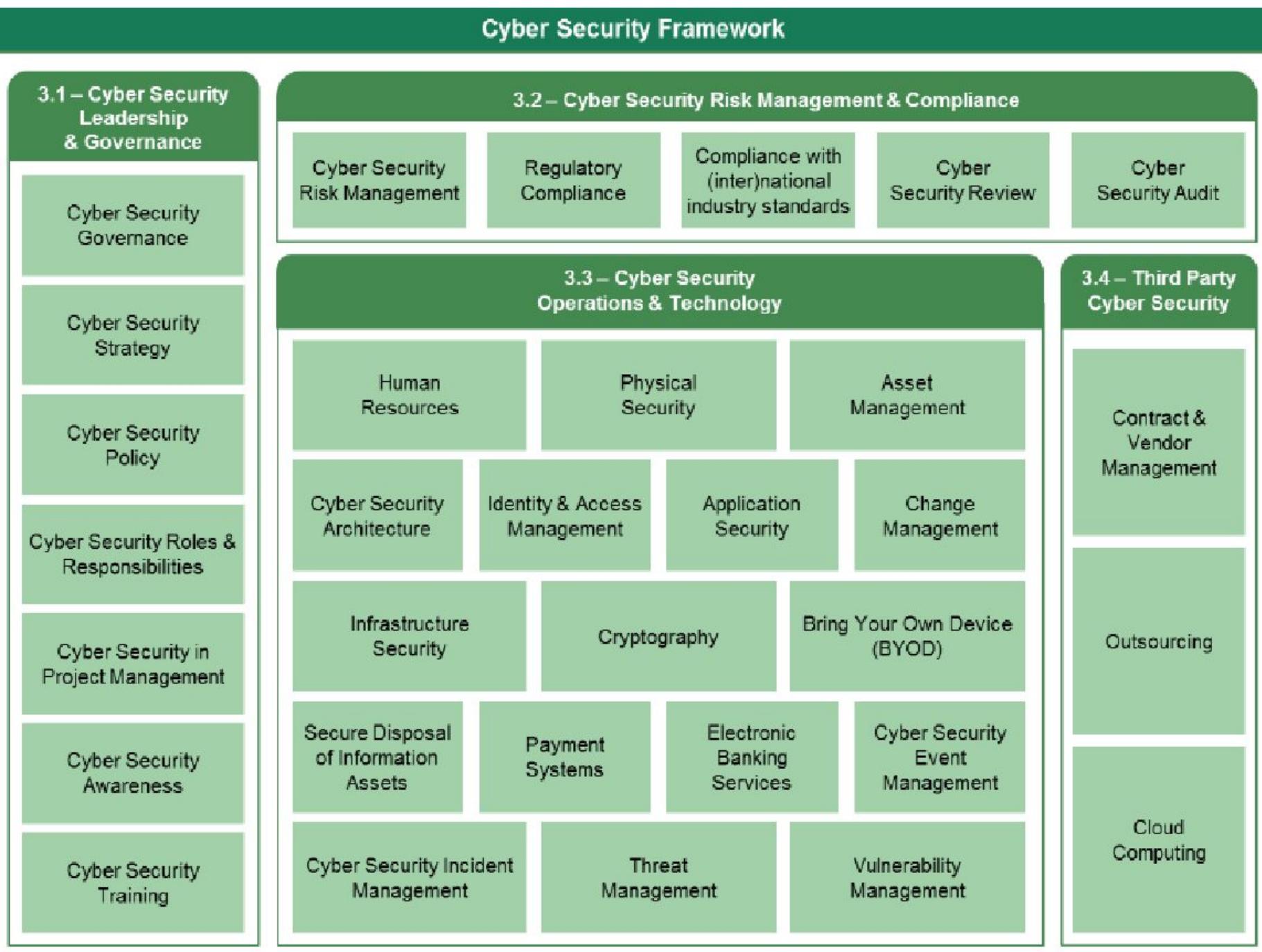


Cyber Security Framework

- All the financial institutions regulated by SAMA must follow the **cyber security framework**.
- The implementation of the Framework at the Member Organization will be subject to a periodic **self-assessment**.
- The self-assessment will be performed by the Member Organization based on a **questionnaire**.
- The self-assessments will be **reviewed** and **audited** by **SAMA** to determine the level of compliance with the Framework and the cyber security maturity level of the Member Organization



Cyber Security Framework



Cyber Security framework contd..

- The objective of the Framework is to create an effective approach for addressing cyber security and managing cyber security risks within the Financial Sector.



Components of cyber security framework

- Cyber security leadership and Governance
- Cyber security risk management and compliance
- Cyber security operations and technology
- Third party cyber security



Cyber security leadership and Governance

- The ultimate responsibility for cyber security rests with the board of the Member Organization.
- The board of the Member Organization can delegate its cyber security responsibilities to a cyber security committee (or a senior manager from a control function).
- The cyber security committee could be responsible for defining the cyber security governance, cyber security strategy and cyber security policy of the member organization.



Cyber security leadership and Governance contd..

1. Cyber security governance: A governance structure should be established and endorsed by the board of directors.
2. Cyber security strategy: A strategy should be setup related to cyber security, which aligns with the organization's strategic objectives.
3. Cyber security policy: A policy should be defined , approved and communicated to all stakeholders.



Cyber security leadership and Governance

contd..

4. Cyber security roles and responsibilities : Responsibilities to implement, maintain, support and promote cyber security should be defined throughout the Member Organization. Additionally, all parties involved in cyber security should understand and take their role and responsibilities.

- There can be a cyber security committee for approving communicating and supporting security strategy and policies.
- A senior management for ensuring standards , processes and security requirements.
- A Chief ISO for implementing and maintaining security policies and strategies. A internal audit team to perform cyber audits. And
- all the members in the organization to comply with security standards and policies of the organization.



Cyber security leadership and Governance contd..

5. Cyber Security in Project Management : ensure that the all the Member Organization's projects meet cyber security requirements.
6. Cyber Security Awareness : A cyber security awareness program should be defined and conducted for staff, third parties and customers of the Member Organization.
7. Cyber Security Training : Staff of the Member Organization should be provided with training regarding how to operate the Member Organization's systems securely and to address and apply cyber security controls.



Cyber Security Risk Management and Compliance

- Risk management is the ongoing process of identifying, analyzing, responding and monitoring and reviewing risks.
- The cyber security risk management process focusses specifically on managing risks related to cyber security.



Cyber Security Risk Management and Compliance contd..

1. Cyber Security Risk Management : A cyber security risk management process should be defined, approved and implemented, and should be aligned with the Member Organization's enterprise risk management process.
2. Cyber Security Risk Identification: Cyber security risk identification should be performed and should include the Member Organization's relevant assets, threats, existing controls and vulnerabilities
3. Cyber Security Risk Response : The cyber security risks of a Member Organization should be treated.
4. Regulatory Compliance : A process should be established by the Member Organization to identify, communicate and comply with the cyber security implications of relevant regulations.



Cyber Security Risk Management and Compliance contd..

5.Compliance with (inter)national industry standards : The Member Organization should comply with mandatory (inter)national industry standards. E.g. It should comply with PCI – DSS (chapter 15)

6.Cyber security review : The cyber security status of the Member Organization's information assets should be subject to periodic cyber security review.

7.Cyber Security Audits :The cyber security status of the Member Organization's information assets should be subject to thorough, independent and regular cyber security audits performed in accordance with generally accepted auditing standards and SAMA cyber security framework



Cyber Security Operations and Technology

- In order to safeguard the protection of the operations and technology of the Member Organization's information assets and its staff, third parties and customers, the Member Organizations have to ensure that security requirements for their information assets and the supporting processes are defined, approved and implemented.



Cyber Security Operations and Technology contd..

- 1. Human Resources:** The Member Organization should incorporate cyber security requirements into human resources processes
- 2. Physical Security:** The Member Organization should ensure all facilities which host information assets are physically protected against intentional and unintentional security events.
- 3. Asset Management:** The Member Organization should define, approve, implement, communicate and monitor an asset management process, which supports an accurate, up-to-date and unified asset register.
- 4. Cyber Security Architecture:** The Member Organization should define, follow and review the cyber security architecture, which outlines the cyber security requirements in the enterprise architecture and addresses the design principles for developing cyber security capabilities



Cyber Security Operations and Technology contd..

- 5. Identity and Access Management:** The Member Organization should restrict access to its information assets in line with their business requirements based on the need-to-have or need-to-know principles.
- 6. Application Security:** The Member Organization should define, approve and implement cyber security standards for application systems. The compliance with these standards should be monitored and the effectiveness of these controls should be measured and periodically evaluated
- 7. Change Management:** The Member Organization should define, approve and implement a change management process that controls all changes to information assets. The compliance with the process should be monitored and the effectiveness should be measured and periodically evaluated
- 8. Infrastructure Security:** The Member Organization should define, approve and implement cyber security standards for their infrastructure components. The compliance with these standards should be monitored and the effectiveness should be measured and periodically evaluated.



Cyber Security Operations and Technology contd..

9. Cryptography: The use of cryptographic solutions within the Member Organizations should be defined, approved and implemented

10. Bring Your Own Device (BYOD): When the Member Organization allows the use of personal devices (e.g., smartphones, tablets, laptops) for business purposes, the use should be supported by a defined, approved and implemented cyber security standard, additional staff agreements and a cyber security awareness training

11. Secure Disposal of Information Assets: The information assets of the Member Organization should be securely disposed when the information assets are no longer required



Cyber Security Operations and Technology contd..

- 12. Payment Systems:** The Member Organization should define, approve, implement and monitor a cyber security standard for payment systems. The effectiveness of this process should be measured and periodically evaluated.
- 13. Electronic Banking Services:** The Member Organization should define, approve, implement and monitor a cyber security standard for electronic banking services. The effectiveness of this standard should be measured and periodically evaluated.
- 14. Cyber Security Event Management:** The Member Organization should define, approve and implement a security event management process to analyze operational and security loggings and respond to security events. The effectiveness of this process should be measured and periodically evaluated.



Cyber Security Operations and Technology contd..

15. Cyber Security Incident Management: The Member Organization should define, approve and implement a cyber security incident management that is aligned with the enterprise incident management process, to identify, respond to and recover from cyber security incidents. The effectiveness of this process should be measured and periodically evaluated.

16. Threat Management: The Member Organization should define, approve and implement a threat intelligence management process to identify, assess and understand threats to the Member Organization information assets, using multiple reliable sources. The effectiveness of this process should be measured and periodically evaluated.



Cyber Security Operations and Technology contd..

17. Vulnerability Management: The Member Organization should define, approve and implement a vulnerability management process for the identification and mitigation of application and infrastructural vulnerabilities. The effectiveness of this process should be measured and the effectiveness should be periodically evaluated.



Third Party Cyber Security

- When Member Organizations do rely on, or have to deal with third party services, it is key to ensure the same level of cyber security protection is implemented at the third party, as within the Member Organization.



Third Party Cyber Security contd.

1. Contract and Vendor Management: The Member Organization should define, approve, implement and monitor the required cyber security controls within the contract and vendor management process
2. Outsourcing: The Member Organization should define, implement and monitor the required cyber security controls within outsourcing policy and outsourcing process. The effectiveness of the defined cyber security controls should periodically be measured and evaluated
3. Cloud Computing: The Member Organization should define, implement and monitor the required cyber security controls within the cloud computing policy and process for hybrid and public cloud services. The effectiveness of the defined cyber security controls should periodically be measured and evaluated.



Summary

- Discussed the SAMA and CMA related to Financial institutions.
- Cyber security framework defines the framework for financial institutions. All the financial institutions in Saudi need to follow it



References

- 1. “Global financial services regulatory guide” available online at
https://www.bakermckenzie.com/-/media/files/insight/publications/2016/07/guide_global_fsrguide_2017.pdf?la=en
- 2. SAMA “Cyber security framework”, available online from
<http://www.sama.gov.sa/en-US/Laws/BankingRules/SAMA%20Cyber%20Security%20Framework.pdf>



Thank You





الجامعة السعودية الإلكترونية
SAUDI ELECTRONIC UNIVERSITY
2011-1432

Bachelor of Science in
Information Technology
IT409
IT Security and Policies

Security Program and Policies

Principles and Practices

by Sari Stern Greene
Updated 02/2018



Objectives

- Explain the importance of strategic alignment
- Know how to manage information security policies
- Describe information security-related roles and responsibilities
- Identify the components of risk management
- Create policies related to information security policy, governance, and risk management



Understanding Information Security Policies

- The goal of the information security policies is to protect the organization from harm:
 - Policies should be written
 - Policies should be supported by management
 - Policies should help companies align security with business requirements and relevant laws and regulations
- ISO 27002:2013 can provide a framework for developing security policies.



What Is Meant by Strategic Alignment?

- Treating security functions as a business enabler that adds value:
 - It requires recognizes the value of information security,
 - invests in people and processes, and treats security in the same fashion as every other business requirement.
- Recognizing that the true value of information security is protecting the business from harm and achieving organizational objectives.



What Is Meant by Strategic Alignment?

- Two approaches to information security:
 - Parallel approach
 - assigns responsibility for being secure to the IT department, views compliance as discretionary, and has little or no organizational accountability
 - Integrated approach
 - recognizes that security and success are intertwined



User Versions of Information Security Policies

- Policies can serve as teaching documents to influence behavior.
- Document and corresponding agreement should be developed specifically for distribution to the user community.
 - Acceptable Use Policy:
 - users needs to acknowledge that they understand their responsibilities and affirm their individual commitment.



Vendor Versions of Information Security Policies

- Vendors (often referred to as “third parties”) that store, process, transmit, or access information assets.
- Companies should create vendor versions of information security policies.
- Vendor should be required to have controls that meet or, in some cases, exceed organizational requirements
- Policies should be authorized by executive management.
- Policies should be updated on regular basis.



Vendor Versions of Information Security Policies

- Vendors (often referred to as “third parties”) that store, process, transmit, or access information assets.
- Companies should create vendor versions of information security policies.
- Vendor should be required to have controls that meet or exceed organizational requirements.



Vendor Versions of Information Security Policies

- One of the most efficient ways to evaluate vendor security is to provide them with a vendor version of organizational security policies and require them to attest to their compliance.
- The vendor version should only contain policies that are applicable to third parties and should be sanitized as to not disclose any confidential information.



Client Synopsis of Information Security Policies

- Client refers to companies to which the organization provides services.
- A synopsis of the information security policy should be available upon request to clients.
- The synopsis could be expanded to incorporate:
 - Incident response and business continuity procedures
 - Notifications
 - Regulatory cross-references.
- The synopsis should not disclose confidential business information unless the recipients are required to sign a non-disclosure agreement



Evaluating Information Security Policies

- As applicable, standards, guidelines, plans, and procedures must be developed to support the implementation of policy objectives and requirements.
- Any information security policy distributed outside the organization must be sanitized.
- All documentation will be retained for a period of six years from the last effective date.



Who Authorizes Information Security Policy?

- A policy is a reflection of the organization's commitment, direction, and approach and it has four essential practices:
 - Place information security on the Board's agenda.
 - Identify information security leaders, hold them accountable, and ensure support for them.
 - Ensure the effectiveness of the corporation's information security policy through review and approval.
 - Assign information security to a key committee and ensure adequate support for that committee



Revising Information Security Policies: Change Drivers

- Organizations change over time, policies need to be revisited
- Change drivers are events that modify how a company does business and they can be:
 - Demographic
 - Economic
 - Technological and regulatory or personnel related
 - Examples : company acquisition, new products, services or technology, regulatory updates, entering into a contractual obligation, and entering a new market
- Why :
 - Change can introduce new vulnerabilities and risk
 - Changes trigger internal assessment



Evaluating Information Security Policies

- Objective of evaluating information security policy:
 - Measure the effectiveness of a security policy.
 - Estimate adherence to policy directives.
 - Measure the maturity of the information security program.
- Policies can be evaluated internally or by independent third parties.

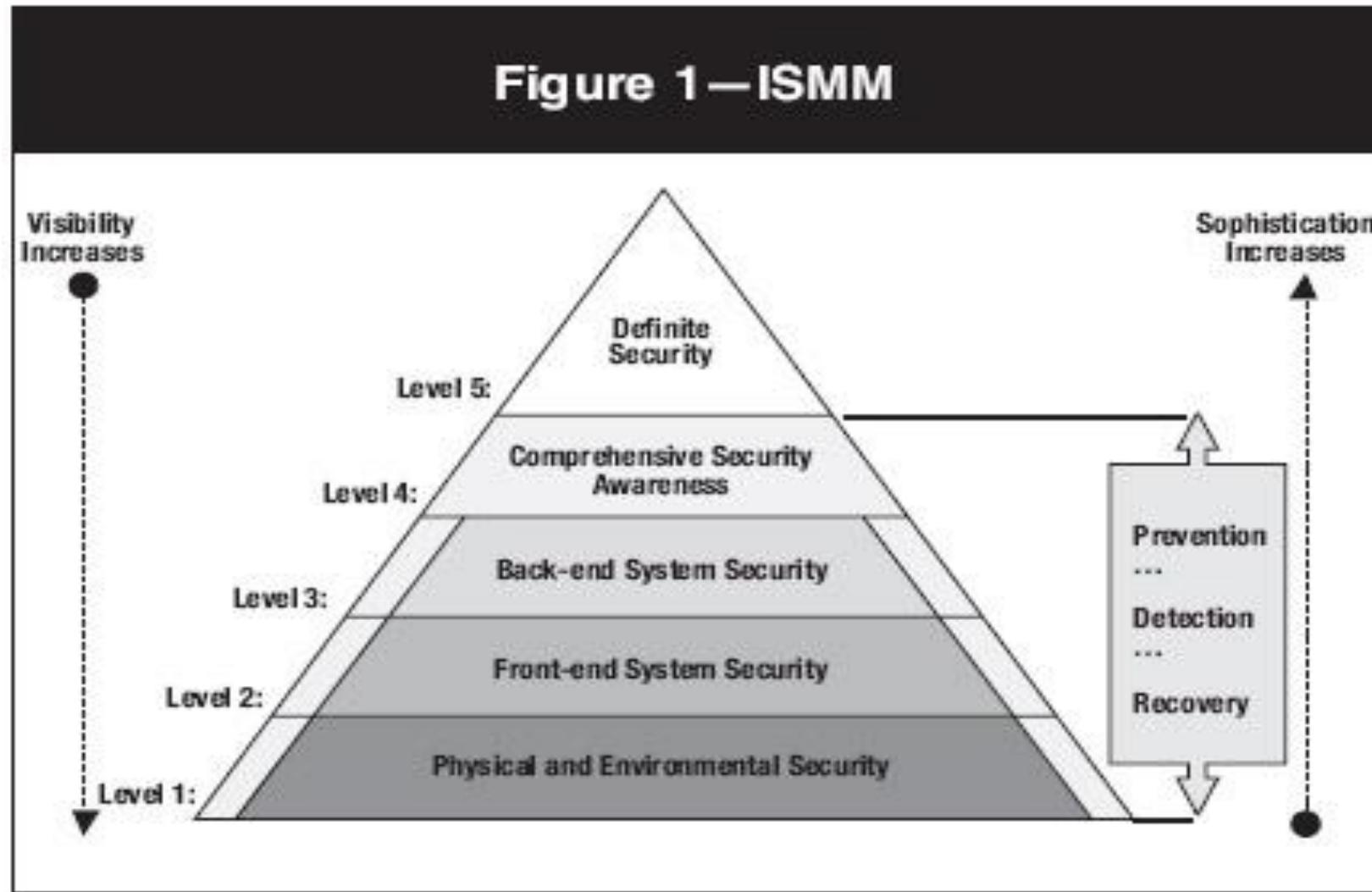


Evaluating Information Security Policies, cont.

- Examples of standardized methodologies to evaluate security policy:
 - Audit:
 - Systematic, evidence-based evaluation.
 - Include interviews, observation, tracing documents to management policies, review or practices, review of documents, and tracing data to source documents.
 - Audit report containing the formal opinion and findings of the audit team is generated at the end of the audit.
 - Capability Maturity Model (CMM):
 - Used to evaluate and document process maturity for a given area.



CMM example



Capability Maturity Model Scale

Level	State	Description
0	Non-Existent	The organization is unaware of need for policies and processes
1	Ad-hoc	There are no documented policies or processes; there is sporadic activity.
2	Repeatable	Policies and processes are not fully documented; however, the activities occur on a regular basis.
3	Defined Process	Policies and processes are documented and standardized; there is an active commitment to implementation
4	Managed	Policies and processes are well defined, implemented, measured, and tested.
5	Optimized	Policies and process are well understood and have been fully integrated into the organizational culture.



Information Security Governance

- The process of managing, directing, controlling, and influencing organizational decisions, actions, and behaviors
- The Board of Directors is usually responsible for overseeing the policy development
- Effective security requires a distributed governance model with the active involvement of stakeholders, decision makers, and users



Distributed Governance Model

- The foundation is the principle that stewardship is an organizational responsibility
- Effective security requires the
 - Active involvement
 - Cooperation
 - Collaboration of stakeholders
 - Decision makers, and the user community



Distributed Governance Model

- Chief information security officer (CISO)
- Information security steering committee
- Compliance officer
- Privacy officer
- Internal audit
- Incident response team
- Data owners
- Data custodians
- Data users



Chief information security officer (CISO)

- The CISO coordinates and manages security efforts across the company, including IT, human resources (HR), communications, legal, facilities management, and other groups.
 - The COO will appoint the CISO.
 - The CISO will report directly to the Chief Operating Officer (COO).
 - At his or her discretion, the CISO may communicate directly with members of the Board of Directors.
 - The CISO will chair the Information Security Steering Committee.



Information Security Steering Committee

- The Information Security Steering Committee (ISC) is tasked with supporting the information security program:
 - serves in an advisory capacity.
 - provides an open forum to discuss business initiatives and security requirements.
 - Standing membership will include the CISO (Chair), the COO, the Director of Information Technology, the Risk Officer, the Compliance Officer, and business unit representatives.
 - will meet on a monthly basis.



Organizational Roles and Responsibilities

- In addition to the CISO and the Information Security Steering Committee, a variety of roles that have information security–related responsibilities:
 - Compliance Officer - Responsible for identifying all applicable information security–related statutory, regulatory, and contractual requirements.



Organizational Roles and Responsibilities

- Privacy Officer - Responsible for the handling and disclosure of data as it relates to state, federal, and international law and customs.
- Internal audit - Responsible for measuring compliance with Board-approved policies and to ensure that controls are functioning as intended.
- Incident response team - Responsible for responding to and managing security-related incidents.



Organizational Roles and Responsibilities

- Data owners - Responsible for defining protection requirements for the data based on classification, business need, legal, and regulatory requirements; reviewing the access controls; and monitoring and enforcing compliance with policies and standards
- Data custodians - Responsible for implementing, managing, and monitoring the protection mechanisms defined by data owners and notifying the appropriate party of any suspected or known policy violations or potential endangerments.



Organizational Roles and Responsibilities

- Data users - Are expected to act as agents of the security program by taking reasonable and prudent steps to protect the systems and data they have access to.
- These responsibilities should be documented in policies, job descriptions, or employee manuals.



Regulatory Requirements

- Most standards require assigning security-related roles and responsibilities. For example:
- **Payment Card Industry Data Security Standard (PCI DSS) Section 12.5:**
 - “Assign to an individual or team the following information security management responsibilities: establish, document, and distribute security policies and procedures; monitor and analyze security alerts and information, and distribute to appropriate personnel; establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations; administer user accounts, including additions, deletions, and modifications; monitor and control all access to data.”



Information Security Risk

- Three factors influence information security decision making and policy creation:
 - Guiding principles.
 - Regulatory requirements.
 - Risk associated with achieving business objectives.



Information Security Risk, Cont.

- Risk: The potential of undesirable or unfavorable outcome from a given action
- Risk tolerance: How much undesirable outcome the risk taker is willing to accept
- Risk appetite: The amount of risk an entity is willing to accept in pursuit of its mission



Risk Assessment

- Evaluate what can go wrong and the likelihood of a harmful event occurring.
- Risk assessment involves:
 - Identifying the inherent risk based on relevant threats, threat sources, and related vulnerabilities.
 - Determining the impact of a threat if it occurs.
 - Calculating the likelihood of occurrence.
 - Determining residual risk.



Risk Assessment cont.

- Inherent risk:
 - The level of risk before security measure are applied.
- Residual risk:
 - The level of risk after security measures are applied
- Threat:
 - Natural, environmental, or human event that could cause harm.
 - Information security focuses on the threats to:
 - confidentiality (unauthorized use or disclosure)
 - integrity (unauthorized or accidental modification),
 - availability (damage or destruction).



Risk Assessment cont.

- **Vulnerability**
 - A weakness that could be exploited by a threat.
- **Impact**
 - The magnitude of a harm.
- **A threat source is either:**
 - Intent and method targeted at the intentional exploitation of a vulnerability, such as criminal groups, terrorists, and disgruntled employees
 - or a situation and method that may accidentally trigger a vulnerability such as an severe storm, and accidental or unintentional behavior.



Business Risk Categories

- In a business context, risk is further classified by category:
 - Strategic risk relates to adverse business decisions.
 - Financial (or investment) risk relates to monetary loss.
 - Reputational risk relates to negative public opinion.
 - Operational risk relates to loss resulting from inadequate or failed processes or systems.
 - Personnel risk relates to issues that affect morale, productivity, recruiting, and retention.
 - Regulatory/compliance risk relates to violations of laws, rules, regulations, or policy.



Risk Assessment Methodologies

- Components of a risk assessment methodology include:
 - Defined process
 - Assessment approach
 - Standardized analysis
- Three well-known information security risk assessment methodologies
 - Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
 - Factor Analysis of Information Risk (FAIR)
 - NIST Risk Management Framework (RMF)



Risk Management

- The process of determining an acceptable level of risk, calculating the current risk level, accepting the level of risk, or taking steps to reduce it to an acceptable level
 - Risk acceptance
 - Risk mitigation
 - Risk reduction
 - Risk transfer
 - Risk sharing
 - Risk avoidance



Risk Management

- Risk Acceptance: Risk acceptance indicates that the organization is willing to accept the level of risk associated with a given activity or process.
- Risk Mitigation: The process of reducing, sharing, transferring or avoiding risk.
- Risk Reduction: Process of control to lower the residual risk.
 - Offensive Control: reducing or eliminating the vulnerabilities by enhanced training or applying security patch.
 - Defensive control: respond to threat source such as sensor sending an alert or detecting an intruder.



Risk Management

- Risk Transfer: shifts the entire risk responsibility or liability from one organization to another organization. This is often accomplished by purchasing insurance.
- Risk sharing: shifts a portion of risk responsibility or liability to other organizations.
- Risk avoidance: involves taking specific actions to eliminate or significantly modify the process or activities that are the basis for the risk.



Summary

- Information security policies should be reviewed at least annually to ensure they are relevant and accurate
- Information security audits should be conducted to ensure policies are accepted and integrated
- Governance is the process of managing, directing, controlling, and influencing organizational decisions, actions, and behaviors
- Risk management is the process of determining an acceptable level of risk, calculating the current risk level, accepting the level of risk, or taking steps to reduce it to an acceptable level



Thank You





الجامعة السعودية الإلكترونية
SAUDI ELECTRONIC UNIVERSITY
2011-1432

Bachelor of Science in
Information Technology
IT409
IT Security and Policies

Security Program and Policies

Principles and Practices

by Sari Stern Greene
Updated 02/2018



Chapter 2: Policy Elements and Style

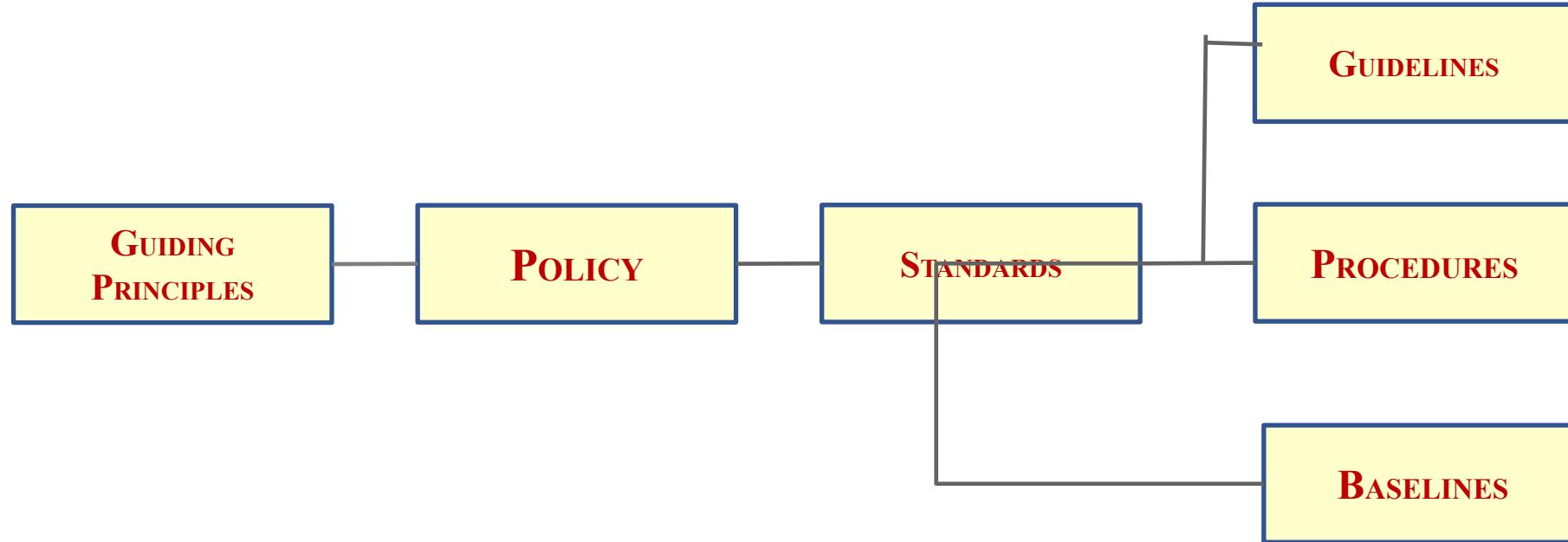


Objectives

- Distinguish between a policy, a standard, a baseline, a procedure, a guideline, and a plan
- Identify policy elements
- Include the proper information in each element of a policy
- Know how to use “plain language”



Policy Hierarchy



Policies reflect the guiding principles and organizational objectives



Policy Hierarchy

- Policies need supporting documents for context and application
 - Standards, baselines, guidelines, and procedures support policy implementation
- The relationship between a policy and its supporting documents is known as the policy hierarchy



Policy Hierarchy cont.

- **Standards**
 - Dictate specific minimum requirements in policies
 - They are specific
 - Determined by management and can be changed without the Board of Director authorization
 - Note that standards change more often than policies
- **Baselines**
 - An aggregate of implementation standards and security controls for a specific category or grouping (for example, Windows 7, smartphones, and so on)



Example of password policy vs. password standard

■ Password policy

- All users must have a unique user ID and password
- Users must not share their password with anyone
- If a password is suspected to be compromised, it must be changed immediately

■ Password standard

- Minimum of 8 upper- and lowercase alphanumeric
- Must include at least one special characters
- Must not include repeating characters ex. 111
- Must not include the user's name, company name



Policy Hierarchy cont.

■ Guidelines

- Suggestions for the best way to accomplish a given task
 - Guidelines are created primarily to assist users in their goal to implement the policy
 - They are not mandatory

■ Procedures

- Method, or set of instructions, by which a policy is accomplished
 - A step-by-step approach to implementation
- Four commonly used formats for procedures
 - Simple step, hierarchical, graphic, flowchart



Example of procedure to change a windows password

- Simple step procedure to change a user's windows password
 - Press and hold the Ctrl+Alt+Delete keys
 - Click the change password option
 - Type your current password in the top box
 - Type your new password in both the second and third boxes
 - Click OK and then log with your new password



Policy Hierarchy cont.

- Plans and Programs
 - Provide strategic and tactical instructions on how to execute an initiative or respond to a situation
 - Plans and programs are used interchangeably
 - Plans are closely related to policies



Policy Format

- The style and format of a policy will change based on the target audience of said policy
 - Identify and understand the audience
 - Identify the culture shared by the target audience
- Plan the organization of the document before you start writing it. Will it be...
 - One document with multiple sections?
 - Consolidated policy section
 - Several individual documents?
 - Singular policy



Policy Components

- **Policy components**
 - Policies include many different sections and components
 - Each component has a different purpose
 - Clearly identify the purpose of each element in the planning phase before the writing part starts



Version Control

- Used to keep track of the changes to the policy
- Usually identified by a number or letter code
- Major revisions advance by a number or letter
 - 1.0, 2.0, 3.0
- Minor revisions advance by a subsection
 - 1.1, 1.2, 1.3
- Version control documentation includes:
 - Change date
 - Name of the person(s) making the change
 - Brief synopsis of the change
 - Who authorized the change
 - The effective date of the change



Introduction

- Provides context and meaning
- Explains the significance of the policy
- Explains the exemption process and the consequences of noncompliance
- Reinforces the authority of the policy
- A separate document for a singular policy
- Follows the version control table and serves as a preface for consolidated policy



Policy Headings

- Identifies the policy by name and provides an overview of the policy topic or category
- The format and content depends on the policy format
 - Singular policy includes:
 - Name of the organization or the division
 - Category, section, and subsection
 - Name of the author and effective date of the policy
 - Version number and approval authority
 - Consolidated policy document
 - Heading serves as a section introduction and includes an overview



Policy Goals and Objectives

- What is the goal of the policy?
- Introduces the employee to the policy content and conveys the intent of the policy
- One policy may have several objectives
- Singular policy objectives are located in the policy heading or in the body of the document
- Consolidated policy objectives are grouped after the policy heading



Policy Statement

- Why does the policy exist?
- What rules need to be followed?
- How will the policy be implemented?



Policy Statement

- High-level directive or strategic roadmap
 - Focuses on the specifics of how the policy will be implemented
 - It's a list of all the rules that need to be followed
 - Constitutes the bulk of the policy
 - Standards, procedures, and guidelines are not a part of the Policy Statement. They can, however, be referenced in that section



Policy Exceptions

- Not all rules are applicable 100% of the time
- Exceptions do not invalidate the rules, as much as they complement them by listing alternative situations
- Language used in this section must be clear, accurate, and concise so as not to create loopholes
- Keep the number of exceptions low



Policy Enforcement Clause

- Rules and penalty for not following them should be listed in the same document
- The level of the severity of the penalty should match the level of severity and nature of the infraction
- Penalties should not be enforced against employees who were not trained on the policy rules they are expected to follow



Administrative Notations

- Provides a reference to an internal resource or refers to additional information
- Include regulatory cross-references, the name of corresponding document (standard, guideline, and so on), supporting documentation (annual reports, job descriptions), policy author name and contact information



Policy Definitions

- ❑ The glossary of the policy document
- ❑ Created and included to further enhance employee understanding of the policy and rules
- ❑ Renders the policy a more efficient document
- ❑ The target audience(s) should be defined prior to the creation of the glossary
- ❑ Useful to show due diligence of the company in terms of explaining the rules to the employees during potential litigation



Writing Style and Technique

- Sets the first impression
- Policies should be written using plain language
 - Simplest, most straightforward way to express an idea
 - Follow The Plain Language Action and Information Network (PLAIN) guidelines



The Plain Language Action and Information Network (PLAIN) guidelines

- Write for your audience
- Write short sentences
- Limit a paragraph to one subject
- Be concise
- Don't use jargon or technical terms
- Use active voice
- Use must not shall
- Use words and terms consistently through your document



Summary

- The structure of the policy documents ease the maintenance and creation of the overall document.
- A successful policy sets forth requirements (standards), ways for employees to act according to the policy (guidelines) and actual procedures.
- A policy is a complex set of individual documents that build upon each other to convey the message to all employees of the organization in an efficient fashion.



Thank You





الجامعة السعودية الإلكترونية
SAUDI ELECTRONIC UNIVERSITY
2011-1432

Bachelor of Science in
Information Technology
IT409
IT Security and Policies

Security Program and Policies

Principles and Practices

by Sari Stern Greene
Updated 02/2018



Chapter 1: Understanding Policy



Objectives

- Describe the significance of policies
- Evaluate the role policy plays in corporate culture and civil society
- Discuss information security policy
- Identify the characteristics of a successful policy
- Discuss Information Security Policy lifecycle



Introduction

- Policy: “A definite course of action or procedure selected from among alternatives and in light of given conditions to guide and determine present and future decisions”**

(** per www.merriam-webster.com)



Looking at Policy Through the Ages

- The role of the Torah and Bible as written policy
 - 3000-year old documents include business rules still in practice today
 - First documented attempt at creating a code to preserve order



Looking at Policy Through the Ages

Cont.

- The U.S. Constitution as a Policy Revolution
 - A collection of articles and amendments that codify all aspects of American government along with citizens' rights and responsibilities
 - A rule set with a built-in mechanism for change
- Both the Constitution and the Torah have a similar goal:
 - Serve as rules that guide behavior



Policy Today

- **Corporate culture**
 - Shared attitudes, values, goals, and practices that characterize a company
 - Three classifications
 - Negative
 - Neutral
 - Positive
- **Guiding principles**
 - Reflect the corporate culture



Information Security Policy

- A **document** that states how an organization plans to **protect** its **information assets** and information systems and ensure compliance with legal and regulatory requirements
 - **Asset**
 - Resource with a value
 - **Information asset**
 - Any information item, regardless of storage format, that represents value to the organization
 - Customer data, employee records, IT information, reputation, and brand



Successful Policy Characteristics

- **Endorsed**
 - Management supports the policy
- **Relevant**
 - The policy is applicable and supports the goals of the organization
- **Realistic**
 - The policy makes sense
- **Attainable**
 - The policy can be successfully implemented
- **Adaptable**
 - The policy can be changed
- **Enforceable**
 - Controls that can be used to support and enforce the policy exist
- **Inclusive**
 - The policy scope includes all relevant parties

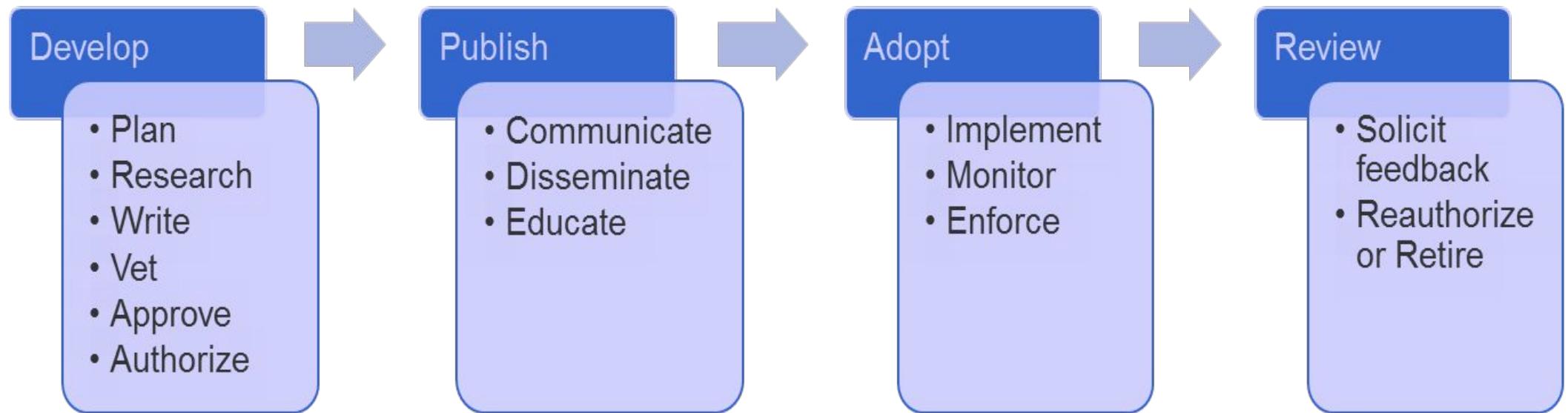


Defining the Role of Policy in Government

- Government regulation is required to **protect** its critical infrastructure and citizens
- Two major information security-related legislations were introduced in Saudi Arabia
 - **Anti-Cyber Crime ACT.**
 - <http://www.citc.gov.sa/en/RulesandSystems/CITCSYSTEM/Pages/CyberCrimesAct.aspx>
 - **Electronic Transactions ACT**
 - <http://www.citc.gov.sa/en/RulesandSystems/CITCSYSTEM/Pages/ElectronicTransactionsLaw.aspx>



Information Security Policy Lifecycle



Information Security Policy Lifecycle cont.

Regardless of the type of policy, its success depends on how the organization approaches the process of development, publishing, adopting and reviewing the policy.

1) **Policy development:** There are six main tasks involved in policy development:

- a) **planning** – identifying the need and context of the policy,
- b) **researching** –defining legal, regulatory requirements,
- c) **writing** – making a document according to the audience,
- d) **vetting-** examining,
- e) **approving** – by all concerned department, and
- f) **authorizing-** approval from the management.



Information Security Policy Lifecycle cont.

- 2) **Policy Publication:** Policies should be communicated and made available to all parties they apply to. The company should provide training to reinforce the policies. Creating a culture of compliance can ensure all parties understand the importance of the policy and actively support it.
- 3) **Policy Adoption:** The policy is implemented, monitored, and enforced.
- 4) **Policy Review:** Policies are reviewed annually, and outdated policies are updated or retired.



Summary

Policies apply to governments as well as to business organizations.

When people are grouped to achieve a common goal, policies provide a framework that guides the company and protects the assets of that company.

The policy lifecycle spans four phases: develop, publish, adopt, and review.



Thank You



Security Program and Policies

Principles and Practices

by Sari Stern Greene
Updated 02/2018



Objectives

- Explain access control fundamentals
- Apply the concepts of default deny, need-to-know, and least privilege
- Understand secure authentication
- Protect systems from risks associated with Internet connectivity, remote access, and telework environments
- Manage and monitor user and administrator access
- Develop policies to support access control management



Access Control Fundamentals

- Access controls
 - Security features that govern how users and processes communicate and interact with systems and resources
 - Primary objective is to protect information and systems from unauthorized access, modification, or disruption
- Three common attributes of access controls
 - **Identification scheme** – identifies unique records in the set, subject supplies identifier to the object
 - **Authentication method** – how identification is proven to be genuine
 - **Authorization method** – the process of assigning authenticated subjects the permission to carry out a specific operation.



What Is a Security Posture?

- The **security posture** of an organization **determines** the default settings for **access controls**
- Access controls can be:
 - **Technical** (such as firewalls or passwords),
 - **Administrative** (such as separation of duties or dual controls), or
 - **Physical** (such as locks, bollards, or turnstiles).



What Is a Security Posture?

- Two fundamental security postures:
 - Open
 - which implements the “**default allow**” model
 - means that access, not explicitly forbidden, is permitted.
 - Secure,
 - which implements the “**default deny**” model
 - means that access, not explicitly permitted, is forbidden.
- Every access control decision for a company is based on that company’s security posture



What Is a Security Posture? Cont.

- Default allow versus default deny
 - Default allow: By default, out-of-the-box, no security is deployed, everyone can do everything
 - Easier to deploy, works out-of-the-box
 - No security
- Default deny
 - Aka “deny all”
 - Access is unavailable by default until the appropriate control is altered to allow access



What Is a Security Posture? Cont.

- Determining who to grant access to should be based on the security principle of **need-to-know**.
- The **level of access required** should be based on the security principle of **least privilege**.
- **Need-to-know** means that the subject has a demonstrated and authorized reason for being granted access to information.
- Once a need-to-know has been established, **least privilege** is the principle of only assigning required object access permissions



What Is a Security Posture? Cont.

■ Principle of Least Privilege

- Definition: The least amount of permissions granted users that still allow them to perform whatever business tasks they have been assigned, and no more.
- This is a strong foundation for any access control policy.
- Protects the data but also protects users. They can't be accused of having deleted a file to which they can't gain access!
- From a cultural stand point, it is important to explain to employees why they are not "trusted" with all the company's data.



What Is a Security Posture? Cont.

■ Need-to-know

- Definition: Having a demonstrated and authorized reason for being granted access to information
- Should be made a part of the company's culture
- Should be incorporated in security training curriculum
- At the least protects the confidentiality of corporate data, but may also protect integrity and availability depending on the attack type



How Is Identity Verified?

- First step to granting access is user identification
 - Authentication: Subject must supply verifiable credentials offered referred as factors
 - Single-factor authentication
 - Multifactor authentication
 - Multilayer authentication



How Is Identity Verified?

- Single-factor authentication:
 - When only one factor is presented. The most common method of single-factor authentication is the password.
- Multifactor authentication:
 - When two or more factors are presented.
- Multilayer authentication:
 - When two or more of the same type of factors are presented.



How Is Identity Verified? Cont.

Three categories of factors

1. **Knowledge**: Something you know

- **Password or PIN**: Passwords are the most commonly used single-factor network authentication method. The authentication strength of a password is a function of its length, complexity, and unpredictability.
- **Answer to a question**: Common examples are mother's maiden name and favorite color.



How Is Identity Verified? Cont.

Three categories of factors

2. **Possession**: Something you have

- **One-time passcodes (OTP)**: is a set of characteristics that can be used to prove a subject's identity one time and one time only
- **Memory cards**: is an authentication mechanism that holds user information within a magnetic strip and relies on a reader to process the information.
- **Smart cards**: Instead of a magnetic strip, it has a microprocessor and integrated circuits.
- **Out-of-band communication**: requires communication over a channel that is distinct from the first factor.



How Is Identity Verified? Cont.

Three categories of factors

3. **Inherence:** Something you are

- **Biometric identification:** is the identification of humans by distinctive, measurable characteristics or traits. A biometric identification system scans an attribute of a person and compares it to a record that was created in an earlier enrollment process.
- **Anatomical attributes:** include fingerprint, finger scan, palm scan, hand geometry, retina scan, iris scan, facial scan, and DNA.
- **Physiological attributes:** includes handwriting, keyboard dynamics, and voice print.

Biometric authentication is the most accurate factor; it is also the most expensive to implement and maintain.



What Is Authorization?

- The process of assigning authenticated subjects permission to carry out a specific operation.
- The authorization model defines how access rights and permission are granted.
- Three primary authorization models
 1. Object capability
 - Used programmatically and based on a combination of a unforgettable reference and an operational message



What Is Authorization?

2. Security labels

- Mandatory access controls embedded in object and subject properties

3. Access Control Lists

- Used to determine access based on some criteria such as a user ID, group membership, classification, location, address, and date.

What Is Authorization? Cont.

- Categories of access control lists
 - **MAC** (Mandatory Access Control): Data is classified, and employees are granted access according to the sensitivity of information
 - **DAC** (Discretionary Access Control): Data owners decide who should have access to what information
 - **RBAC** (Role-based Access Control): Access is based on positions (roles) within an organization
 - **Rule-based** access control: Access is based on criteria that is independent of the user or group account



Infrastructure Access Controls

- Include physical and logical network design, border devices, communication mechanisms, and host security settings
- Network segmentation
 - The process of logically grouping network assets, resources, and applications
 - Type of network segmentation
 - Enclave network
 - Trusted network
 - Semi-trusted network, perimeter network, or DMZ
 - Guest network
 - Untrusted network



Type of Network Segmentation

- Enclave network:
 - A segment of an internal network that requires a higher degree of protection. Internal accessibility is further restricted through the use of firewalls, VPNs, VLANs, and network access control (NAC) devices.
- Trusted network
 - The internal network that is accessible to authorized users. External accessibility is restricted through the use of firewalls, VPNs, and IDS/IPS devices. Internal accessibility may be restricted through the use of VLANs and NAC devices.



Type of Network Segmentation

- Semi-trusted network, perimeter network, or DMZ:
 - A network that is designed to be Internet accessible. Hosts such as web servers and email gateways are generally located in the DMZ. Internal and external accessibility is restricted through the use of firewalls, VPNs, and IDS/IPS devices.
- Guest network:
 - A network that is specifically designed for use by visitors to connect to the Internet. There is no access from the Guest network to the internal trusted network.
- Untrusted network:
 - A network outside your security controls. The Internet is an untrusted network.



What Is Layered Border Security?

- Different types of security measures designed to work in tandem with a single focus – to protect internal network from external threats.
 - Firewall devices
 - Intrusion detection systems (**IDSs**)
 - Intrusion prevention systems (**IPSs**)
 - Content filtering and **whitelisting/blacklisting**
 - Border device administration and management



Layered Border Security? Cont..

Firewalls

- are devices or software that control the flow of traffic between networks. They are responsible for examining network entry and exit requests and enforcing organizational policy.
- are a mandatory security control for any network connected to an untrusted network such as the Internet.
- Without a properly configured firewall, a network is completely exposed and could potentially be compromised within minutes, if not seconds
- The rule set is used by the firewall to evaluate **ingress** (incoming) and **egress** (outgoing) network traffic.



Layered Border Security? Cont..

■ Intrusion detection systems - (IDSs)

- are passive devices designed to analyze network traffic in order to detect unauthorized access or malevolent activity.
- Most IDSs use multiple methods to detect threats, including signature-based detection, anomaly-based detection, and stateful protocol analysis.
- If suspicious activity is detected, IDSs generate an onscreen, email, and/or text alert.

■ Intrusion prevention systems (IPSs)

- are active devices that sit inline with traffic flow and can respond to identified threats by disabling the connection, dropping the packet, or deleting the malicious content



Layered Border Security? Cont..

There are four types of IDS/IPS technologies:

1. Network-based IDS/IPS

- Monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity

2. Wireless IDS/IPS

- Monitors wireless network traffic and analyzes it to identify suspicious activity involving the wireless networking protocols themselves



Layered Border Security? Cont..

3. Network behavior analysis IDS/IPS

- Examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations.

4. Host-based IDS/IPS

- Monitors the characteristics of a single host and the events occurring within that host for suspicious activity



Layered Border Security? Cont..

IDS/IPS has four decision states.

1. **True positive** occurs when the IDS/IPS correctly identifies an issue.
2. **True negative** occurs when the IDS/IPS correctly identifies normal traffic.
3. **False positive** occurs when the IDS/IPS incorrectly identifies normal activity as an issue.
4. **False negative** occurs when the IDS/ISP incorrectly identifies an issue as normal activity.



Layered Border Security? Cont..

Content Filtering and Whitelisting/Blacklisting

- The filters can be supplemented by self-generated, open source, or subscription-based IP whitelists and/or blacklists.
- **Whitelists** are addresses (IP and/or Internet domain names) of known “good” sites to which access should be allowed.
- Conversely, **blacklists** are addresses (IP and/or Internet domain names) of known “bad” sites to which access should be denied. It is common practice to block entire ranges of IP addresses specific to geographic regions.
- **Content-filtering** applications can be used to restrict access by content category (such as violence, gaming, shopping, or pornography), time factors, application type, bandwidth use, and media.



Layered Border Security? Cont..

Border device administration and management

- It is a 24/7/365 responsibility.
- On a daily basis, performance needs to be monitored to enable potential resource issues to be identified and addressed before components become overwhelmed.
- Logs and alerts must be monitored and analyzed to identify threats—both successful and unsuccessful.
- Administrators need to be on the watch for security patches and apply them expediently.



Remote Access Security

■ Remote Access

- Users who have a demonstrated business-need to access the corporate network remotely and are authorized to do so must be given that privilege
- Not all employees should be given this privilege by default
- Remote access activities should be monitored and audited
- The organization's business continuity plan must account for the telecommuting environment



Remote Access Security (Cont.)

- Remote access technologies
 - Virtual Private Networks (VPNs)
 - Secure tunnel for transmitting data over unsecure network, such as the Internet
 - Remote access portals
 - Offers access to one or more applications through a single centralized interface



Remote Access Security (Cont.)

■ Remote Access Authentication and Authorization

- Whenever feasible, organizations should implement mutual authentication so that a remote access user can verify the legitimacy of a remote access server before providing authentication credentials to it.
- Network access control (NAC) systems can be used to “check” a remote access device based on defined criteria such as operating system version, security patches, antivirus software version, and wireless and firewall configurations before it is allowed to connect to the infrastructure.



Remote Access Security (Cont.)

Teleworking Access Controls

- The Telework Enhancement Act of 2010, defines **teleworking** as “a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee’s position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work.”
- In plain language, **teleworking allows employees to work offsite, often from their home.**
- NIST SP 880-114: User’s Guide to Securing External Devices for Telework and Remote Access provides practical, real-world recommendations for securing telework computers’ operating systems (OS) and applications



User Access Controls

- Used to ensure authorized users can access information and resources while unauthorized users cannot access information and resources
- Users **should have access only to information they need to do their job and no more**
- Administrative account controls
 - Segregation of duties
 - Dual control



What Types of Access Should Be Monitored?

- Mining log data results in a **wealth of information** that can be used to **protect** your organization.
- Log data offers **clues** about **activities** that have unexpected and possibly harmful consequences, including the following:
 - **At-risk events**, such as unauthorized access, malware, data leakage, and suspicious activity
 - **Oversight events**, such as reporting on administrative activity, user management, policy changes, remote desktop sessions, configuration changes, and unexpected access
 - **Security-related operational events**, such as reporting on patch installation, software installation, service management, reboots bandwidth utilization, and DNS/DHCP traffic



What Types of Access Should Be Monitored?

- Three main monitoring areas:
 - Successful access
 - record of user activity
 - Reporting should include date, time, and action
 - Failed access
 - indicative of either unauthorized attempts or authorized user issues
 - Privileged operations
 - Compromise or misuse of administrator accounts can have disastrous consequences.



Is Monitoring Legal?

- Employees **should have no expectation of privacy while on company time or when using company resources**
- Courts **have favored an employer's right to protect their interests over individual privacy rights because:**
 - Actions were taken at the employer's place of work
 - Equipment used – including bandwidth – was company-provided
 - Monitoring the work also helps ensure the quality of work
 - The employer has the right to protect property from theft and/or fraud



Is Monitoring Legal? Cont.

- Courts indicate that monitoring is acceptable if it is reasonable:
 - Justifiable if serving a business purpose
 - Policies are set forth to define what privacy employees should expect while on company premises
 - Employees are made aware of what monitoring means are deployed
- Acceptable use agreement should include a clause informing users that the company will and does monitor system activity
- Users must agree to company policies when logging on



Summary

- Access control is a complex domain. Access to information is extremely important to regulate.
- User access and user actions on the network must be **monitored** and **logged**, whether they are located on premises or gaining access to the network remotely.
- Monitoring is useless if the information gathered is not **reviewed regularly**.





الجامعة السعودية الإلكترونية
SAUDI ELECTRONIC UNIVERSITY
2011-1432

Bachelor of Science in
Information Technology
IT409
IT Security and Policies

Security Program and Policies

Principles and Practices

by Sari Stern Greene
Updated 02/2018



Objectives

- Prepare for an **information security incident**
- Identify an information security incident
- Recognize the **stages in incident management**
- Properly **document** an information security incident
- Understand federal and state **data breach notification** requirements
- Consider an incident from the perspective of the victim
- Create policies related to information security incident management



Introduction

- In general terms, incident management is defined as a predictable response to damaging situations.
- It is vital that organizations have the practiced capability to respond **quickly**, **minimize** harm, comply with **breach-related** state laws and federal regulations, and maintain their composure in the face of an unsettling and unpleasant experience.



Organizational Incident Response

- Incidents drain resources and can be expensive
- The right time to develop an Incident Response plan is before an incident occurs
- Incident preparedness includes having policies, strategies, plans, and procedures
 - The benefits of having a practiced incident response capability include the following:
 - Calm and systematic response
 - Minimization of loss or damage
 - Protection of affected parties
 - Compliance with laws and regulations
 - Preservation of evidence
 - Integration of lessons learned
 - Lower future risk and exposure



What Is an Incident?

- Information security incident is an adverse event that threatens business security and/or disrupts service
- Difference between security **incident** and **disaster**
- Every organization should be familiar with and prepared to respond to the following core group of attacks
 - Intentional unauthorized access or use
 - Occurs when an insider or an intruder gains logical or physical access without permission



What Is an Incident? Cont.

- Denial of service (DoS) attacks
 - Prevents or impairs the normal authorized functionality of the organization's networks, systems, or applications
- Malware
 - Code that is covertly inserted into another program with the intent of gaining authorized access or causing harm
- Inappropriate usage
 - Occurs when authorized user performs actions that violate company policy, agreement, law, or regulation



Incident Severity Levels

- Three severity levels
 - Level 1
 - Incidents that could cause significant harm
 - Level 2
 - Compromise of or unauthorized access to noncritical systems or information
 - Level 3
 - Situations that can be contained and resolved by the information system custodian, data/process owner, or HR personnel



TABLE 11.1 Incident Severity Level Matrix

An information security incident is any adverse event whereby some aspect of an information system or information itself is threatened. Incidents are classified by severity relative to the impact they have on an organization. Each level has a maximum response time and minimum internal notification requirements.

Severity Level = 1

Explanation	Level I incidents are defined as those that could cause significant harm to the business, customers, or the public and/or are in violation of corporate law, regulation, or contractual obligation.
Required Response Time	Immediate.
Required Internal Notification	Chief Executive Officer. Chief Operating Officer. Legal counsel. Chief Information Security Officer. Designated incident handler.
Examples	Compromise or suspected compromise of protected customer information. Theft or loss of any device or media on any device that contains legally protected information. A denial of service attack. Identified connection to "command and control" sites. Compromise or suspected compromise of any company website or web presence. Notification by a business partner or vendor of a compromise or potential compromise of a customer or customer-related information. Any act that is in direct violation of local, state, or federal law or regulation.



Severity Level = 2

Explanation	Level 2 incidents are defined as compromise of or unauthorized access to noncritical systems or information; detection of a precursor to a focused attack; a believed threat of an imminent attack; or any act that is a potential violation of law, regulation, or contractual obligation.
Required Response Time	Within four hours.
Required Internal Notification	Chief Operating Officer. Legal counsel. Chief Information Security Officer. Designated incident handler.
Examples	Inappropriate access to legally protected or proprietary information. Malware detected on multiple systems. Warning signs and/or reconnaissance detected related to a potential exploit. Notification from a third party of an imminent attack.

Severity Level = 3

Explanation	Level 3 incidents are defined as situations that can be contained and resolved by the information system custodian, data/process owner, or HR personnel. There is no evidence or suspicion of harm to customer or proprietary information, processes, or services.
Required Response Time	Within 24 hours.
Required Internal Notification	Chief Information Security Officer. Designated incident handler.
Examples	Malware detected and/or suspected on a workstation or device, with no external connections identified. User access to content or sites restricted by policy. User's excessive use of bandwidth or resources.



How Are Incidents Reported?

- Employees should be required to report all actual and suspected incidents
- The employee who discovers an incident may not be trained or an IT technician
- The culture of the company needs to incorporate this point so that employees don't feel like they may be ridiculed if they are wrong



What Is an Incident Response Program

- Composed of policies, plans, procedures, and people
- An incident response plan (IRP) is a roadmap of reporting, responding, and recovery actions
- Incident response procedures are detailed steps needed to implement the plan



What Is an Incident Response Program Cont.

- **Activities in the IRP**

- Preparation
- Detection and investigation
- Initial response
- Containment
- Eradication and recovery
- Notification
- Closure and post-incident activity
- Documentation and evidence-handling requirements



What Is an Incident Response Program Cont.

- **Preparation** includes developing internal incident response capabilities, establishing external contracts and relationships, defining legal and regulatory requirements, training personnel, and testing plans and procedures.
- **Detection and investigation** include establishing processes and a knowledge base to accurately detect and assess precursors and indicators. A **precursor** is a signal or warning that an incident may occur in the future. An **indicator** is substantive or corroborating evidence that an incident may have occurred or may be occurring now. Indicators are sometimes referred to as IOCs (indicators of compromise).



What Is an Incident Response Program Cont.

- **Initial response** include incident declaration, internal notification, activation of an incident response team, and/or designated incident handlers, and prioritization of response activities.
- **Containment** includes taking the steps necessary to prevent the incident from spreading, and as much as possible limit the potential for further damage.
- **Eradication and recovery** include the elimination of the components of the incident (for example, malicious code, compromised passwords), addressing the vulnerabilities related to the exploit or compromise, and restoring normal operations.



What Is an Incident Response Program Cont.

- **Notification** includes the steps taken to notify state and federal agencies, affected parties, victims, and the public-at-large.
- **Closure and post-incident activity** include incident recap, information sharing, documentation of “lessons learned,” plan and procedure updates, and policy updates and risk reviews, as applicable.
- **Documentation and evidence-handling requirements** include the recording of facts, observations, participants, actions taken, forensic analysis, and evidence chain of custody. Although the primary reason for gathering evidence during an incident is to resolve the incident, it may also be needed for subsequent risk assessments, notifications, and legal proceedings.



Key Incident Management Personnel

- **Incident response coordinator (IRC)**
 - Central point of contact for all incidents
 - Verifies and logs the incident
- **Designated incident handlers (DIHs)**
 - Senior-level personnel who have crisis management and communication skills, experience, and knowledge to handle an incident
- **Incident response team (IRT)**
 - Trained team of professionals that provide services through the incident lifecycle



Key Incident Management Personnel contd.

- Tasks assigned to the IRT include but are not limited to the following:
 - Overall management of the incident
 - Triage and impact analysis to determine the extent of the situation
 - Development and implementation of **containment** and **eradication** strategies
 - Compliance with **government** and/or other **regulations**
 - Communication and follow-up with **affected parties** and/or individuals
 - Communication and follow-up with other **external parties**, including the Board of Directors, business partners, government regulators (including federal, state, and other administrators), law enforcement, representatives of the media, and so on, as needed
 - Root cause analysis and lessons learned
 - Revision of policies/procedures necessary to prevent any recurrence of the incident



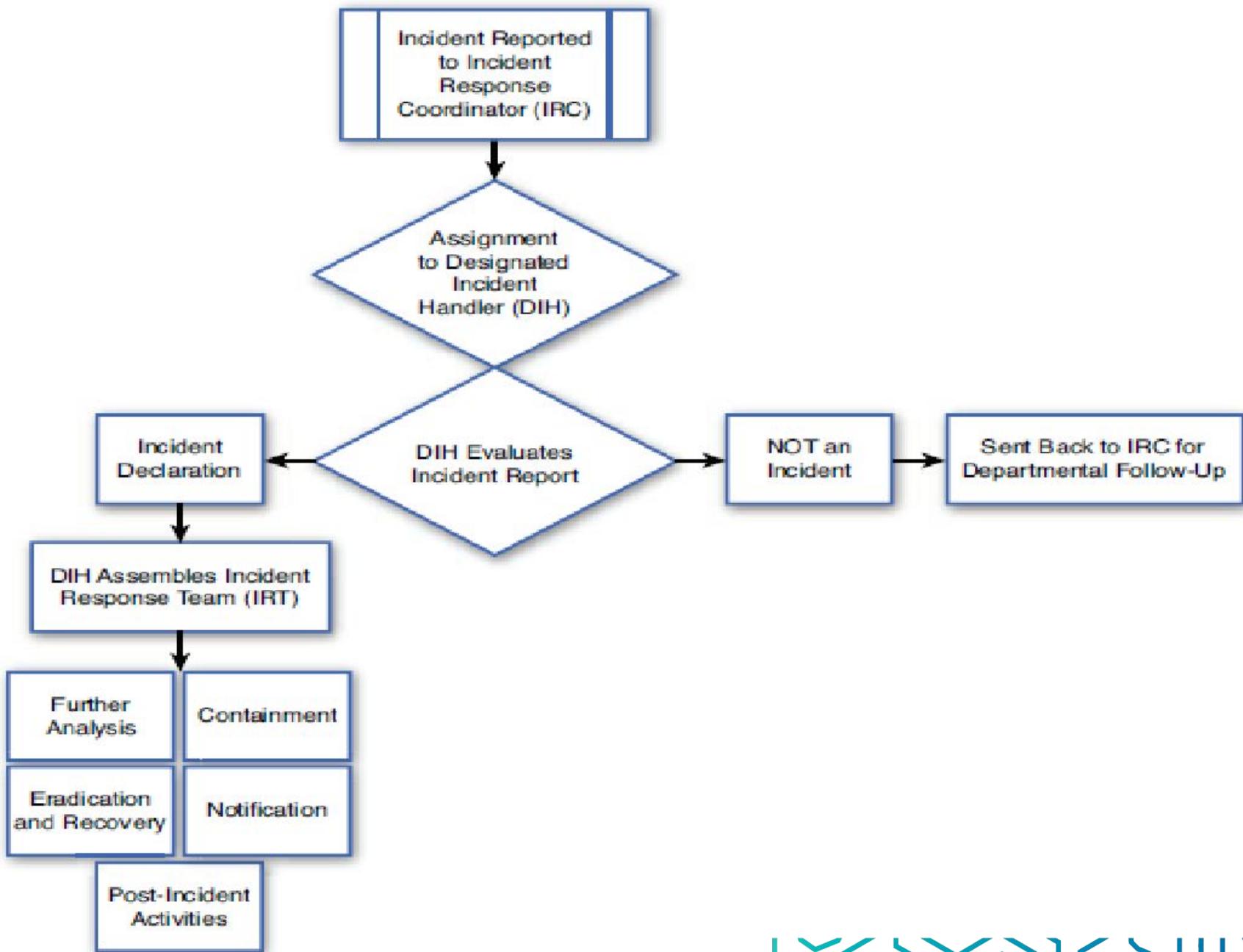


FIGURE 11.1 Incident response roles and responsibilities.



Communicating Incidents

- Throughout the incident lifecycle, there is frequently the need to communicate with outside parties, including law enforcement, insurance companies, legal counsel, forensic specialists, vendors, external victims, and other IRTs.



Incident Response Training and Exercises

- Establishing a robust response capability ensures that the organization is prepared to respond to an incident swiftly and effectively.
- Responders should receive training specific to their individual and collective responsibilities. Recurring tests, drills, and challenging incident response exercises can make a huge difference in responder ability.



Investigation and Evidence Handling

- Incidents should be thoroughly documented
- Documenting Incidents
 - The initial documentation should create an incident profile. The profile should include the following:
 - How was the incident detected?
 - What is the scenario for the incident?
 - What time did the incident occur?
 - Who or what reported the incident?
 - Who are the contacts for involved personnel?
 - A brief description of the incident.
 - Snapshots of all on-scene conditions.



Working with law enforcement

- Depending on the incident it may be necessary to contact local, state, or federal law enforcement
 - The IRT team should be acquainted with applicable law enforcement representatives
- Incident handlers that perform **forensic analysis** should be familiar with forensic principles, guidelines, procedures, tools, and techniques



Investigation and Evidence Handling cont.

- The process of **digital forensic** includes
 - Collection
 - Examination
 - Analysis
 - Reporting
- Chain of custody applies to physical, digital, and forensic **evidence**
 - It is used to prove that evidence has not been altered
- Evidence should be stored in a secure location



Investigation and Evidence Handling cont.

- To maintain an evidentiary chain, a **detailed log** should be maintained that includes the following information:
 - Where and when (date and time) evidence was discovered
 - Identifying information such as the location, serial number, model number, hostname, media access control (MAC) address, and/or IP address
 - Name, title, and phone number of each person who discovered, collected, handled, or examined the evidence
 - Where evidence was stored/secured and during what time period
 - If the evidence has changed custody, how and when the transfer occurred (include shipping numbers, and so on).



Investigation and Evidence Handling cont.

- **Storing and Retaining Evidence**
- It is not unusual to retain all evidence for months or years after the incident ends. **Evidence, logs, and data** associated with the **incident** should be placed in tamper-resistant containers, grouped together, and put in a limited-access location. Only incident investigators, executive management, and legal counsel should have access to the storage facility.



Data Breach Notification Requirements

- **Definition :** A data breach is widely defined as an **incident** that results in compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or unauthorized use or loss of control of legally protected PII (**Personally identifiable information**), including the following:
 - Any information that can be used to distinguish or trace an individual's identity, such as name, SSN, date and place of birth, mother's maiden name, or biometric records.
 - Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.



Data Breach Notification Requirements

contd.

- Information that is standing alone is not generally considered personally identifiable, because many people share the same trait, such as first or last name, country, state, ZIP Code, age(without birthdate), gender, race, or job position.
- However, multiple pieces of information ,none of which alone may be considered personally identifiable, may uniquely identify a person when brought together.



Is there a government breach notification law?

- The short answer is, there is not.
- Consumer information breach notification requirements have historically been determined at the state level.
- There are, however **regulations** that require certain regulated sectors (such as healthcare, financial, and investment) to protect certain types of personal information, implement information security programs, and provide notification of security breaches.



Personal Healthcare Information (PHI)

- Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual. [ISO/IEC 2382-8].
- In the context of the Saudi HIE (**Health information Exchange**), it refers to an individual's interest in limiting who has access to personal healthcare information.
- As per MOH Portal kingdom of Saudi Arabia **Information** about an identifiable person which relates to the physical or mental **health** of the individual, or to provision of health services to the individual, and which may include:



Personal Healthcare Information (PHI) Cont.. As per MOH Portal KSA

- a) information about the registration of the individual for the provision of health services.
- b) information about payments or eligibility for healthcare with respect to the individual;
- c) a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes;
- d) any information about the individual collected in the course of the provision of health services to the individual;
- e) information derived from the **testing or examination of a body part or bodily substance**;
- f) identification of a person (e.g., a health professional) as provider of healthcare to the individual. [ISO 27799]



Personal Healthcare Information (PHI) Cont..

- Definitions related to PHI :
- Date use agreement : Comprehensive agreement that governs the exchange of health data between participants in the Saudi Health Information Exchange.
- Health record: Repository of information regarding the health of a subject of care. [ISO 13606-1] Under this policy, this refers to all personal health information accessible through the Saudi Health Information Exchange.



Personal Healthcare Information (PHI) Cont..

- Definitions related to PHI :
- Privacy and security audit : Audit focused on assuring conformance to privacy and security practices and procedures.
- Sensitive PHI : PHI Subject to heightened confidentiality requirements (at least including but not limited to mental health, substance abuse, genetic information, sexually transmitted disease, reproductive health).



Data Breach Notification

- The **data breach** notification in healthcare must include the following:
- a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known,
- a description of the types of PHI that were involved in the breach (such as full name, national identification number, date of birth, home address, etc.),



Data Breach Notification Cont..

- the steps individuals should take to **protect** themselves from potential **harm** resulting from the breach,
- a brief description of what the PHCS(Participating Health care Subscriber) and the Saudi Health Information Exchange are doing to further investigate the breach, to **mitigate** harm to individuals, and to protect against any further breaches, and
- contact procedures for individuals to ask questions or learn additional information, which SHALL include a telephone number, an e-mail address, a web site, or postal address.



Does Notification Work?

- In June 2012, Experian commissioned the Ponemon Institute to conduct a consumer study on data breach notification. The findings are instructive. When asked “What personal data if lost or stolen would you worry most about?”, they overwhelmingly responded “password/PIN” and “Social Security number.”
- Consumers trust those who collect their personal information to protect it. When that doesn’t happen, they need to know so that they can take steps to protect themselves from identity theft, fraud, and privacy violations.



Does Notification Work?

- Eighty-five percent believe notification about data breach and the loss or theft of their personal information is relevant to them.
- Fifty-nine percent believe a data breach notification means there is a high probability they will become an identity theft victim.
- Fifty-eight percent say the organization has an obligation to provide **identity protection services**, and 55% say they should provide credit-monitoring services.



Summary

- An information security **incident** threatens business security and disrupts **operations**. Examples of incidents include **unauthorized access**, **DoS attacks**, **malware**, and **inappropriate usage**.
- Companies should have an incident response **plan** that details how incidents should be handled and the roles and responsibilities of key personnel.
- In most situations **data breaches** of PII should be reported to the appropriate authority and affected parties notified.



Thank You

