

## CompTIA CASP+

Created By: Margaret Grigor, Teaching Assistant

### Module 1: Risk Management

#### Lesson 1.3: Risk Management (02:01)

*Skills Learned From This Lesson: Definitions, Objectives, and CLOP*

- Risk Management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. It is forward-looking.
- Objectives: Understanding Security Concepts, Threats/Vulnerabilities, and Risk Management
- CLOP: Controlling, Leading, Organizing and Planning It is the four functions of the management process.

#### Lesson 1.4: Understanding Security Concepts Part 1(10:45)

*Skills Learned From This Lesson: CIA TRIAD, Who Implements It, Acceptance of Risk, and Different Types of Risks*

- CIA TRIAD
  - Confidentiality- Protects and ensures that data or an information system is accessed by only an authorized person.
  - Integrity- The principle of integrity asserts that information and functions can be added, removed or altered only by authorized people.
  - Availability- This is the final component of the CIA Triad and refers to the actual availability of the data. Authentication mechanisms, access channels, and systems all have to work properly for the information they protect and ensure it's

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

---

available when it is needed.

- Confidentiality
  - Assurance that information can be read, interpreted, or accessed in any way only by persons and processes explicitly authorized to do so.
  - Protecting confidentiality involves implementing procedures and measures to prevent malicious and accidental disclosure of information to unauthorized users.
- Integrity
  - Assurance that the information remains intact, accurate and authentic.
  - Protecting integrity involves preventing and detecting unauthorized creation, modification, or destruction of data.
- Availability
  - Assurance that authorized users can access and work with information assets, resources, and systems when needed, with sufficient response and performance.
  - Protecting availability involves measures to sustain accessibility to information in spite of possible sources of interference, including system failures and deliberate attempts to obstruct availability.

## Who Implements the C-I-A Triad?

### Confidentiality

- User
- IT administrator
- Network administrator
- Human resources
- Senior management

### Integrity

- User
- IT administrator
- Network administrator
- Human resources
- Senior management

### Availability

- IT administrator
- Network administrator
- Third-party vendor, for example, ISP

- Classifying Assets- An asset is any data, device, or other components of the environment that supports information-related activities. Assets can be tangible. It generally includes hardware, software, and confidential information. Assets can be intangible, which is, and not have a physical presence like corporate image, intellectual

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

property, and patents.

- Threats- Any circumstance/event with the potential to harm an information resource by exploiting vulnerability such as natural, unintentional, intentional-physical or non-physical threats.
- Risk is an inherent part of the business. All risks cannot be eliminated and every organization has to accept a level of risk.
- Risk Appetite- The level of risk that an organization is prepared to accept in pursuit of its objectives, and before action is deemed necessary to reduce the risk.
- Acceptable Risk- Determine an optimal point where the cost of loss intersects with the cost of mitigation. It is the probability and impact of a particular risk.

## Lesson 1.5: Understanding Security Concepts Part 2 (11:28)

*Skills Learned From This Lesson: Vulnerabilities Defined, Calculate Risk, and Premises Defined*

- Vulnerabilities are referred to as a flaw or any type of weakness in a computer system, in a set of procedures, or in anything that leaves information security exposed to a threat.
- Identification of risks is the first step is to generate a comprehensive list of threat sources, risks, and events that impact the achievement of each of the objectives identified in the definition of scope and framework. Risk can be related to or characterized by various factors.
- Defense in Depth- It means layers of security to defend your assets. If one mechanism fails the next layer reacts to thwart off an attack of the data.
- Countermeasures- Any process that serves to counter specific threats and be considered a targeted control. Security countermeasures are used to protect the confidentiality, integrity, and availability of data and systems (CIA TRIAD).

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Residual Risk

- Definition:
- **Residual risk** is the risk that remains after you apply controls. It's not feasible to eliminate all risks. Instead, you take steps to reduce the risk to an acceptable level. The risk that's left is residual risk.
  - $\text{Risk} = \text{Threat} \times \text{Vulnerability}$
  - $\text{Total risk} = \text{Threat} \times \text{Vulnerability} \times \text{Asset Value}$
- You can calculate residual risk with the following formula:
  - $\text{Residual Risk} = \text{Total Risk} - \text{Controls}$
- Senior management is responsible for any losses due to residual risk. They decide whether a risk should be avoided, transferred, mitigated or accepted. They also decide what controls to implement. Any resulting loss due to their decisions falls on their shoulders.
- Physical Security- Keep in mind several goals like authentication, access control, and auditing.
- Physical premises have three logical areas: external, internal perimeters and secured areas.
  - External Perimeter Security is the first line of defense surrounding the organization. A common security measure you may encounter with respect to the organization's external perimeter includes security cameras, badge readers, etc.
  - Internal Security Perimeter- It starts with building walls and exterior doors and includes any internal security measures, with the exception of secure areas within the building. Some features used may be locks, indoor security cameras, guard desk, etc.
  - Secure Areas- Has limited access to internal employee access and not accessed by the third party. Examples would be badge readers, keypads, etc.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

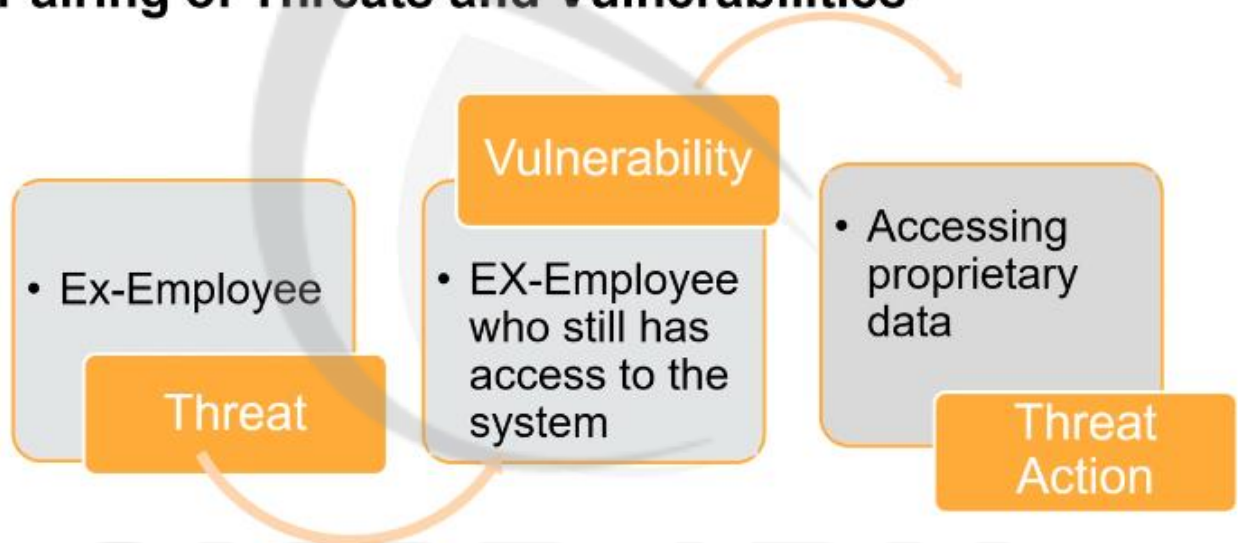
---

## Lesson 1.6: Understanding Threats and Vulnerabilities

*Skills Learned From This Lesson: Threats, Pairing, and Importance of Risk Management*

- Threats refer to anything that has the potential to cause serious harm to a computer system. A threat is something that may or may not happen, but has the potential to cause serious damage.

- ### Pairing of Threats and Vulnerabilities



- Importance of Risk Management- It identifies threats and vulnerabilities, reduces adverse impact, improves organization survivability, enhances cost-benefit awareness and shows the need for risk reduction.

## Lesson 1.7: Understanding Risk Assessment Part 1 (13:14)

*Skills Learned From This Lesson: Metrics, KRIs and KRIs, Analysis Security Solutions, and Critical Components*

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

---

- Risk Assessment- A systematic process of evaluating the potential risks that can negatively impact your organization.
- Metric- Standards of measurement by which efficiency, performance, progress, quality of a plan, process, or product can be assessed.

## What Do We Measure to Get the Metrics?

- Security program performance against quantifiable objectives
  - Trends –external and internal risk factors targeted by security programs
  - Accountability –the diligence of line business unit managers to protect against known risks
  - Change –relationship of security programs to an improved state of risk management
  - Benchmarks –how are we doing vs. our peers?
  - Value assessment, cost management, ROI, budget burn rates, etc.
  - The “hygiene” of the firm –business conduct, continuity, integrity, etc.
  - Security’s effectiveness as rated by customers
  - Performance measurement of staff, others
  - What happened? Lessons-learned, case results, end game statistics
  - Project implementation status
  - Defect reduction
- 
- Key Risk Indicators KRI’s- This is a metric that provides information on the level of exposure to a given operational risk which the organization has at a particular point in time.
  - Key control Effectiveness Indicators KCIs- Are metrics that provide information on the extent to which a given control is meeting its intended objectives (in terms of loss prevention, reduction, etc.)
  - Key Performance Indicators KPIs- Are metrics that measure performance or the achievement of targets.
  - 14 Step Approach to KRIs and KPIs
    - Step 1. Understand the business context.
    - Step 2. Identify audiences and collaborates.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

---

- Step 3. Determine common interests.
  - Step 4. Identify key information security priorities.
  - Step 5. Design KPI/KRI combinations.
  - Step 6. Test and confirm KPI/KRI combinations.
  - Step 7. Gather data.
  - Step 8. Produce and calibrate KPI/KRI combinations.
  - Step 9. Interpret KPI/KRI combinations to develop insights.
  - Step 10. Agree to conclusions proposals and recommendations.
  - Step 11. Produce reports and presentations.
  - Step 12. Prepare to present and distribute reports.
  - Step 13. Present and agree on the next steps.
  - Step 14. Develop learning and improvement plans.
- Benchmark versus Baselines- A benchmark is a point of reference later used for comparison, captures the same data as a baseline and can even be used as a new baseline should the need arise. A baseline is a reference point that is defined and captured to be used as a future reference.
  - Good Metrics are Smart which means the following:
    - S= Specific
    - M= Measurable
    - A= Attainable
    - R=Repeatable
    - T=Time-Dependent
  - Analyzing Security Solutions
    - 1. Performance is the manner in which or the efficiency with which a device or technology reacts or fulfills its intended purpose.
    - 2. Latency is delay typically incurred in the processing of network data. A low-latency network connection is one that generally experiences short delay times, while a high-latency connection generally suffers from long delays.
    - 3. Scalability is a characteristic of a device or security solution that describes its capability to cope and perform under an increased or expanding workload. Scalability is generally defined by time factors.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- 4. Capability is the action that the solution is able to perform. For example, an intrusion detection system (IDS) detects intrusions, whereas intrusion prevention systems (IPS) prevent intrusions.
  - 5. Usability means making security solutions or devices easier to use and matching the solution or device more closely to organizational needs and requirements.
  - 6. Maintainability is how often a security solution or device must be updated and how long the updates take.
  - 7. Availability is the amount or percentage of time a computer system is available for use. When determining availability, the following terms are often used: maximum tolerable downtime (MTD), mean time to repair (MTTR) and mean time between failures (MTBF).
  - 8. Recoverability is the probability that a failed security solution or device can be restored to its normal operable state within a given time frame using the prescribed practices and procedures.
  - 9. Cost/Benefit Analysis is performed before deploying any security solutions to the enterprise. This type of analysis compares the cost of deploying a particular solution to the benefits that will be gained from its deployment.
- Quantitative Risk Assessments- It can help in determining any specific types of risks to focus on events that need to be handled in the near-term or long term effects. Will calculate absolute financial values, losses, and costs.
  - Qualitative Risk Assessments- It is a technique used to quantify the risk associated with a particular risk. This calculates relative values, losses, and costs.
  - Risk Management and Its Importance to Organization
    - Identify the IT assets of an organization and its value. This can include data, hardware, software, services, and IT infrastructure.
    - Identify threats and vulnerabilities to these assets. Prioritize the threats and vulnerabilities.
    - Identify the likelihood a vulnerability will be exploited.
    - Identify the impact of a risk. Risks with higher impacts should be addressed sooner as you prioritize them.
  - Critical Components of Risk Assessment



---

# CYBRARY

---

- Determine the scope of assessment: view, outlook, application, operation, and effectiveness.
- Identify boundaries of assessment.
- Isolate crucial areas of focus.

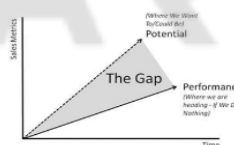
## Lesson 1.8: Understanding Risk Assessment Part 2 (10:13)

*Skills Learned From This Lesson: Steps of Risk Assessment, Gap Analysis, Annual Loss Expectancy, and Single Loss Expectancy*

- Steps of Risk Assessment
  - Risk Identification isolates potential risks to the organization.
  - Risk Analysis analyzes the types of risk to the organization.
  - Risk Prioritization places risks in an order of hierarchy.
- The importance of risk assessment is part of the overall risk management process, helps evaluate controls, supports decision making and can help organizations remain in compliance.
- Gap Analysis- It is an examination of your current performance for the purpose of identifying the differences between your current state of business and where you'd like to be. The purpose is to identify gaps between your current management systems and establish a list of actions to achieve conformance with the standard.

### Gap Analysis

- Four (4) Step Process
  - 1. Identify your current state.
  - 2. Identify your desired state.
  - 3. Identify the gaps in your organization.
  - 4. Devise improvements to close the gaps.
- Steps in Gap Analysis
  - Facility walk-through
  - Document review
  - Staff interviews
  - Identify and document gaps



---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- A review of risk assessments should be done when new equipment, new procedures, new substances, annually as rule of thumb or when there is any significant change.

## Annualized loss expectancy

- The **annualized loss expectancy** (ALE) is the product of the annual rate of occurrence (ARO) and the single **loss expectancy** (SLE). It is mathematically expressed as: Suppose that an asset is valued at \$100,000, and the Exposure Factor (EF) for this asset is 25%
- The Annualized Loss Expectancy (ALE) is the expected monetary loss that can be expected for an asset due to a risk over a one year period. It is defined as:
- $ALE = SLE * ARO$
- SLE is the Single Loss Expectancy and ARO is the Annualized Rate of Occurrence.
- An important feature of the Annualized Loss Expectancy is that it can be used directly in a cost-benefit analysis. If a threat or risk has an ALE of \$5,000, then it may not be worth spending \$10,000 per year on a security measure which will eliminate it.

## Single loss expectancy

- Single-loss expectancy is the monetary value expected from the occurrence of a risk on an asset. It is related to risk management and risk assessment. Single-loss expectancy is mathematically expressed as: Where the exposure factor is represented in the impact of the risk over the asset, or percentage of asset lost.
- The Single Loss Expectancy (SLE) is the expected monetary loss every time a risk occurs. The Single Loss Expectancy, Asset Value (AV), and exposure factor (EF) are related by the formula:
- $SLE = AV * EF$
- Introducing this conceptual breakdown of Single Loss Expectancy into Asset Value and Exposure Factor allows us to adjust the two terms independently: Asset Value may vary with inflation, market changes, etc. while introducing preventive measures may enable us to reduce an Exposure Factor.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Module 2: Vulnerability Management

Lesson 2.1: Cybersecurity Research Part 1 (08:21)

*Skills Learned From This Lesson: OWASP Top 10 Security Vulnerabilities, Threat Overview Model, and What's Threat Modeling*

- OWASP Top 10 Security Vulnerabilities
  - 1. Cross-Site Scripting (XSS)- XSS flaws occur whenever an application takes user-supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.
  - 2. Injection Flaws- Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
  - 3. Malicious File Execution- Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.
  - 4. Insecure Direct Object Reference- A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
  - 5. Cross-Site Request Forgery(CSRF)- A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks.
  - 6. Information Leakage and Improper Error Handling- Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data or conduct more serious attacks.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- 7. Broken Authentication and Session Management- Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other user's identities.
  - 8. Insecure Cryptographic Storage- Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes such as card fraud.
  - 9. Insecure Communications- Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.
  - 10. Failure to Restrict URL Access- Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.
- Threat Intelligence- It is knowledge of a threat's capabilities, infrastructure, motives, goals, and resources. Threat intelligence enables you to identify and contextualize your adversaries. Once you understand your adversary, you can take decisive action to better protect your organization.

## Threat Modeling Overview

- Threat modeling consists of Assets, Threats and Attacks
  - Assets are what you want to protect
  - Threats live forever; they are the attacker's goal
  - Attacks are how an attacker can realize a threat
  - Vulnerabilities are design or implementation errors that allow an attack to succeed
- Very hard to write secure solutions unless you understand your Assets, Threats and Attacks
- If done right, provides more ROI than any other security activity



Vulnerabilities are  
unmitigated threats

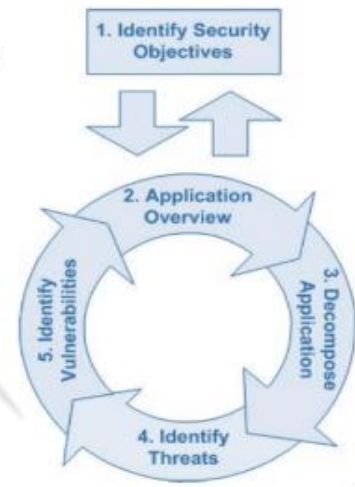
Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## What is Threat Modeling?

- A powerful way to identify potential threats, visualize risk and understand the security of the software system
- Multi-disciplinary effort in which all team members think about and address threats
  - A way for architects to realize and mitigate design problems
  - A road map for developer to write secure code
  - A starting point to create robust security minded test plans
- The most reliable way to:
  - Understand the security implications of system architecture
  - Find business-process and system-level security issues
  - Ensure you get the most impact for your security investment



### Lesson 2.2: Cybersecurity Research Part 2 (06:08)

*Skills Learned From This Lesson: Why Threat Model, Threat Modeling, in A Nutshell, RFC (Request for Comments), and Threat Model- Summarizing Enterprise Risk*

- Why Threat Model?
  - Creates a common understanding amongst technical and management stakeholders
  - Ensures design and code is written to protect critical assets
  - Allows the organization to:
    - Make better decisions throughout development
    - Prioritize security efforts according to true risk
    - Understand your organization's weakness
    - Weigh security designs against functional design goals
    - Step into the mind of an attacker and identify attack vectors

Brought to you by:

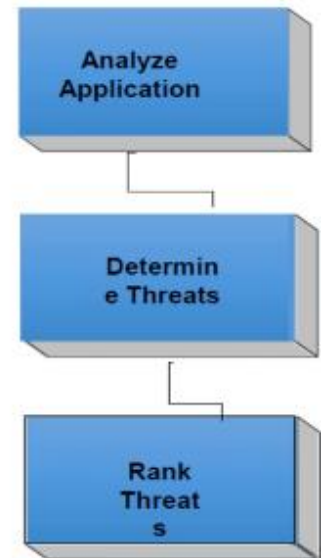
**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.



## Threat Modeling in a Nutshell

- Understand architecture and security requirements
- Identify assets and roles
- Build an activity matrix
- Identify threats that put assets at risk
- Define a set of attacks and/or negative scenarios that could be used to realize threats
- Identify testable conditions each attack requires to be successful
- Assess probability, harm, priority, and business impact of each threat
- Devise mitigations



- Threat Model- Summarizing Enterprise Risk
  - Threat Modeling allows you to get ahead of and plan for risk
  - If you understand threats and risks before deployment, you can reduce security impacts to development schedule and cost
- Most solutions make tradeoffs between security and functionality
  - If low priority security concerns are mis-prioritized, you can negatively impact usefulness and user experience
  - If high priority security concerns are mis-prioritized, you can negatively impact your users and business
- Threat modeling helps you plan and prioritize effectively.
- Threat rating is a quantitative measure of your network's threat level after IPS mitigation. The formula for Threat Rating= Risk Rating- Alert Rating
- RFC (Request for Comments) is a pure technical document published by the Internet Engineering Task Force (IETF).

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

---

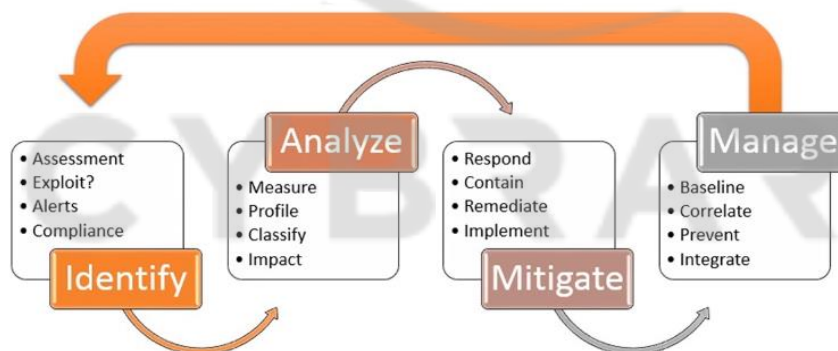
- Request for Comments (RFC) is mainly used to develop a “standard” network protocol, a function of a network protocol or any feature which is related to network communication.

## Lesson 2.3: Vulnerability Assessment Part 1 (05:52)

*Skills Learned From This Lesson: Vulnerability Assessment Defined, Vulnerability Tools, and Vulnerability Techniques*

- Assessing Vulnerabilities is the first step in any security protection plan that begins with an assessment of vulnerabilities. A variety of techniques and tools can be used in evaluating the levels of vulnerability.
- A vulnerability assessment is a systematic and methodical evaluation of asset exposure to attackers, forces of nature, endpoints, poorly written policies and procedures of an organization or any potentially harmful entity.
- Aspects of vulnerability assessment include asset identification, threat evaluation, vulnerability appraisal, risk assessment, and risk mitigation.

### Vulnerability assessment



- Banner Grabbing Tools
  - Banner: a message that a service transmits when another program connects to it. An example would be a banner for an HTTP service that will typically show the type of server software, version number, when it was last modified, and other similar information.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- Banner grabbing: when a program is used to intentionally gather this information. It can be used as an assessment tool to perform an inventory on the services and systems operating on a server.
- Protocol Analyzers
  - Hardware or software that captures packets to decode and analyze contents, also known as a sniffer.
  - Common uses are by network administrators for troubleshooting, characterizing network traffic and security analysis. It can be used to fine-tune the network and manage bandwidth.
- Honeypots defined by SANS.org as fake computer systems set up as a "decoy", which are used to collect data on intruders. It is loaded with bogus information, administrative controls, and a fake network system.
- Honeynet defined by SANS.org as a network, where all inbound and outbound data is analyzed and collected. Within this network, a wide variety of standard production systems are re-established. These systems provide real services, so they more closely match the actual conditions found in an organization but it is totally fake. It is more like a collection of honey pots networked together.

## Lesson 2.4: Vulnerability Assessment Part 2 (05:46)

*Skills Learned From This Lesson: Vulnerability Scanning, Penetration Testing, and Different Types of Penetration Testing*

- Two important vulnerability assessment procedures:
  - Vulnerability scanning
  - Penetration scanning



## Differences between vulnerability scans and penetration tests

	Vulnerability scan	Penetration test
Frequency	At least quarterly, especially after new equipment is loaded or the network undergoes significant changes	Once or twice a year, as well as anytime the Internet-facing equipment undergoes significant changes
Reports	Provide a comprehensive baseline of what vulnerabilities exist and what changed since the last report	Concisely identify what data was compromised
Focus	Lists known software vulnerabilities that could be exploited	Discovers unknown and exploitable weaknesses in normal business processes
Performed by	Typically conducted by in-house staff using authenticated credentials; does not require a high skill level	Best to use an independent outside service and alternate between two or three; requires a great deal of skill
Value	Detects when equipment could be compromised	Identifies and reduces weaknesses

- Vulnerability scanning is an automated software search through a system for known security weaknesses. Creates reports of potential exposures and compared against baseline scans.
- Changes are investigated. Usually performed from inside the security perimeter and does not interfere with normal network operations. Two different methods are performed:
  - Intrusive vulnerability scans- attempts to actually penetrate the system to perform a simulated attack.
  - Non- intrusive vulnerability scan- uses only available information to hypothesize the status of the vulnerability.
- Credentialed vulnerability scan provides credentials (username and password) to the scanner so tests for additional internal vulnerabilities can be performed.
- non-credentialed scans do not use credentials.
- Penetration testing is designed to exploit system weaknesses. Tests are conducted outside the perimeter. Usually done by an independent contractor. It may disrupt

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the *fastest growing catalog* in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

network operations.

- It has three different techniques to deploy a penetration test:
  - Black box testing- the tester has no prior knowledge of the network infrastructure.
  - White box testing- the tester has in-depth knowledge of network and systems being tested.
  - Gray box testing- some limited information has been provided to the tester.

## Lesson 2.5: Vulnerability Assessment Part 3 (08:20)

*Skills Learned From This Lesson: Third-Party Integration, Terms of Agreement, Security Posture, and Effective Security Posture*

- Third-party integration combines system and data with outside entities The risk of third integration include:
  - On-boarding: the start-up relationship between partners
  - Off-boarding: the termination of such an agreement
- Application and social media network sharing. Consideration with the sharing is privacy, risk awareness, and data loss should be considered.
- The terms of understanding is a means by which parties can reach an understanding of their relationships and responsibilities is through interoperability agreements, which include: Service Level Agreement (SLA), Blanket Purchase Agreement (BPA), Memorandum of Understanding (MOU), and Interconnection Security Agreement (ISA).
- Mitigating and deterring attacks have standard techniques. Examples are creating a security posture, selecting and configuring controls, hardening, and reporting.
- Security posture describes an approach, philosophy, or strategy regarding security. Elements that make up a security posture:
  - Initial baseline configuration
    - Standard security checklist
    - Systems evaluated against the baseline
  - Continuous security monitoring
    - Regularly observe systems and networks
  - Remediation

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- As vulnerabilities are exposed, put a plan in place to address them
- Configuring controls properly can be a key to mitigating and deterring attacks.
  - Some controls are for detection. Example: security cameras
  - Some controls are for prevention. Example: properly positioned security guard
  - Information security controls. Configuration to detect attacks and sound alarms, or prevent attacks
- Additional Considerations is when normal functions are interrupted by failure. Which is a higher priority, security or safety?
  - Fail-open locks unlock doors automatically upon failure
  - The fail-safe lock automatically locks- highest security level
  - Firewall can be configured in fail-safe or fail-open state
- Hardening is to eliminate as many risks as possible. Types of hardening techniques include:
  - Protecting accounts with passwords
  - Disabling unnecessary accounts
  - Disabling unnecessary services
  - Protecting management interfaces and applications
- Reporting is important to provide information regarding events that occur so action can be taken.
  - Alarms or alerts sounding a warning if the specific situation is occurring. Example: alert if too many failed password attempts
  - Reporting can provide information on trends. It can indicate a serious impending situation. Example: multiple users accounts experiencing multiple password attempts

## Lesson 2.6: Vulnerability Management (09:40)

*Skills Learned From This Lesson: Vulnerability Management, Reasons for Vulnerability Management, and Different Cycles of Vulnerability Management*

- Vulnerability management is the process in which vulnerabilities in IT are identified and risks are evaluated. The evaluation leads to correcting and removing the risk or formal risk acceptance by the management of an organization (e.g. in case the impact of an

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

attack would be low or the cost correction does not outweigh possible damages to the organization).

- Vulnerability scanning consists of using a computer program to identify vulnerabilities in networks, computer infrastructure or applications.
- Vulnerability management is required to address the increasing growth of cyber-crime or associated risks to information security. The vulnerability management process should be part of an organization's effort to control information security risks.
- The vulnerability management process is to detect and remediate vulnerabilities in a timely fashion. Any vulnerabilities not detected after a scheduled scan takes place will only be detected on the next scan.
- The preparation phase is the first phase of the vulnerability management process. The first step is to define the scope of vulnerability management process and the last step consists of planning the vulnerability scans, Depending on the scan configuration which includes the number of vulnerability checks, authentication scan type, and applications installed on the target, a vulnerability scan against a single IP address can take between a few minutes to a few hours.
- Vulnerability scan detects system weaknesses in computers, networks, and communications equipment and predicts the effectiveness of countermeasures. Most vulnerability scanning tools offer a wide range of reporting options to visualize scan results.
- Remediate action should be executed in line with agreed timeframes. If a problem occurs, it should be recorded. Alternative actions should be defined by the asset owner based on recommendations by the security officer and IT department. The security officer should track the status of the remedial action.
- Rescan may be scheduled to verify the remedial actions are effective. The scan is usually informed with the same scanning tools with identical configurations to compare with the initial scan and to prevent any inaccurate results.

---

*Brought to you by:*

**CYBRARY** | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

## Vulnerability Management Life Cycle



### Module 3: Organizational Security

#### Lesson 3.1: Security Frameworks (10:35)

*Skills Learned From This Lesson: Defined Security Framework, Regulatory Compliance, and Different Key Frameworks*

- The security framework is a series of documented processes that are used to define policies and procedures on the implementation and ongoing management of the security controls of the IT environment.
- The point of having a security framework is to reduce risk levels and the organization's exposure. It is the go-to document in an emergency and outlines daily procedures to reduce your exposure to risk.

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- Regulatory compliance is an organization's adherence to laws regulations, guidelines, and specifications relevant to its business processes. Violations of regulatory compliance regulations often result in legal action including federal fines.
- Choosing the framework that works in your organizations based on the organizational type, risk, and view from top management. Choose a simplified security policy framework domain model that also meets regulatory compliance. Frameworks should be flexible and allow the organization to adapt to fit the need for overall governance and compliance requirements.

## Security Policy Framework- Business Risks



- NIST Cybersecurity Framework stands for the National Institute of Standards and Technology. It is a federal agency within the United States Department of Commerce. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity facilitates trade and improves the quality of life.
- ISO 27000 series is the International Standards Organization. ISO2700 series has a broad scope so any type or size organization can benefit and adopt its recommendations as it fits your needs based on industry and business type. It is also a systematic approach to managing sensitive information securely also known as ISMS. It includes managing risk for people, processes and IT systems.
- ISO 2700 series defines security policy, the scope of the ISMS, risk assessment, manage identified risks, select control objectives and controls to be implemented, and

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

---

prepare a statement of applicability.

- PCI DSS is the worldwide Payment Card Industry Data Security Standard. It was initiated to ensure businesses process card payments were secure, as well as to help reduce card fraud. This encompasses tight controls surrounding storage, transmissions, and processing of the cardholder's data. The payment standard has 12 principle requirements covered in six categories:
  - Build and maintain a secure network
  - Protect card data
  - Maintain a vulnerability program
  - Implement strong access control measures
  - Regularly monitor and test networks
  - Maintain an information security policy
- NIST SP 800-53 is set standards and guidelines to help federal agencies and contractors meet the requirements set by the Federal Information Security Management Act (FISMA). The 800 series reports on the Information Technology Laboratory's (ITL) research and guidelines.
- AICPA Trust Services Principles and Criteria (SOC) is a set of controls that are utilized in SOC2 and SOC3 engagement. It is a set of five trust principles with a focus on Security, Confidentiality, Processing Integrity, and Privacy.
- COBIT stands for Control Objectives for Information and Related Technology. It is a framework created by ISCA (Information Systems Audit and Control Association) for IT governance and management. It was designed to be a supportive tool for managers. It allows bridging the crucial gap between technical issues, business risks, and control requirements. COBIT is a thoroughly recognized guideline that can be applied to any organization in any industry. Overall, COBIT ensures quality, control, and reliability of information systems in an organization, which is also the most important aspect of every modern business.
- ITIL stands for Information Technology Infrastructure Library, is a set of detailed practices for IT service management that focuses on aligning IT services with the needs of the business. It is a framework of best practices for delivering IT services.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

---

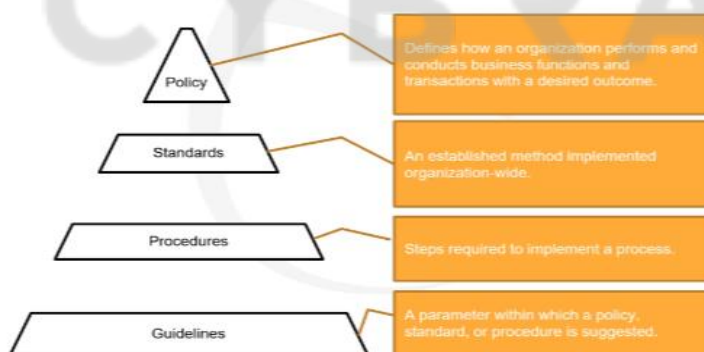
- The Open Group Architecture Framework (TOGAF) is a framework for enterprise architecture that provides an approach for designing, planning, implementing, and governing enterprise information technology architecture.

## Lesson 3.2: Security Policies (07:00)

*Skills Learned From This Lesson: Security Policies, Types of Documentation, Security Controls, and Best Practices*

- Security policy is a set of rules defining who is authorized to access what and under which conditions, and the criteria under which such authorization is given or canceled. Security policies define who, what and why regarding the desired behavior, and they play an important role in an organization's overall security posture. The goal is to provide relevant direction and value to the individuals within an organization.
- There are three main types of policies:
  - Organizational (or Master) Policy
  - System-specific Policy
  - Issue-specific Policy
- Types of Security Documentation: policies, standards, procedures, guidelines, and baselines.

### Information Security Controls



---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.



- Baselines specifies the minimum level of security required. All systems in the organization must comply with that minimum. Evaluations are done on a regular basis to discover any major changes.
- The purpose of security is to document in writing how a company plans to protect the company's physical and information technology (IT) assets.
- Policies and procedures are an important and essential component of an organization. Policies are important because they address pertinent issues, such as what constitutes acceptable behavior by employees. Utilizing both policies and procedures during decision-making ensures that employers are consistent in their decisions.
- Best Practices for Policy Maintenance is:
  - Updates and revisions
  - Exceptions and waivers
  - Request from users and management
  - Changes in the organization

## Lesson 3.3: Document and Operate Security Controls (03:31)

### *Skills Learned From This Lesson: Different Types, Definitions, and Documentation*

- Different types of controls: deterrent, preventive, detective, corrective and compensating controls.
- Definition of controls:
  - Deterrent controls are to prevent specific actions by influencing choices of would-be intruders.
  - Preventive controls are blocks or control specific events.
  - Detective controls are to monitor and record specific types of events.
  - Corrective controls are post-event controls to prevent recurrence.
  - Compensating controls are to introduce to compensates for the absence or failure of control.
- According to SANS Institute: Security *controls* are documented both a living *document* updated regularly based on changing threats as well as a solid, prioritized program for making fundamental computer *security* defenses a well-understood, replicable,

measurable, scalable, reliable, automatable, and continuous process.

## Lesson 3.4: Participate In Change Management (06:16)

*Skills Learned From This Lesson: Change Control, Configuration Management Plan, Impact Assessments, System Architecture, Patch Management, and SDLC*

- Change control refers to the formal procedures adopted by an organization to ensure that all changes are to the appropriate level of management control.
- Configuration Management Plan describes the configuration management (CM) will be conducted throughout the project lifecycle.
- Security impact assessment is the analysis conducted by qualified staff within an organization to determine the extent to which changes to the information system affect the security posture of the system.
- The system architecture is the conceptual model defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the systems.
- Interoperability describes the extent to which systems and devices can exchange data and interpret that shared data.
- Patch management is the application of software and firmware patches to correct vulnerabilities. Patch management is acquired, tested, distributed, and verified usually regularly to information systems. Sometimes emergency fixes are deployed called a “Hot Fix”.

---

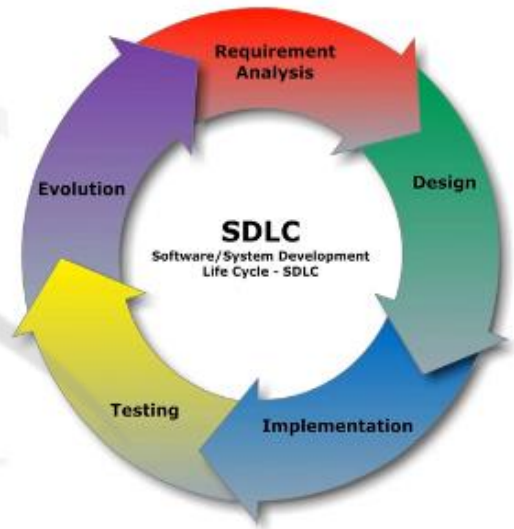
Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Software /System Development Life Cycle

- Requirement gathering and analysis
- Design
- Implementation / Coding
- Testing
- Deployment
- Maintenance



### Lesson 3.5: Participate In Security Awareness and Training (03:50)

*Skills Learned From This Lesson: End-user Awareness, Why Awareness, and Five Areas Awareness*

- People are recognized as being weakness link in protecting your information systems. The purpose of security awareness training is to improve awareness of protecting systems resources, develop skills to perform jobs more securely, and provide awareness to threats to the organization.
- A proactive security awareness program can significantly reduce potential risks by addressing the behavior element of security. Users are the front-line for the risk of threats that not always detectable by automated means.
- Five practical areas to train your employees in security:
  - Physical Security
  - Password
  - Phishing
  - Social Engineering

*Brought to you by:*

**CYBRARY** | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Malware

## Module 4: Applied Cryptography

Lesson 4.2: Understand and Apply Fundamental Concepts of Cryptography (10:49)

*Skills Learned From This Lesson: Cryptography, Hash Functions, Salting, Symmetric Encryption, Digital Signatures, Steganography, and Non-repudiation*

- Cryptography is used to protect at rest and data in motion from being compromised or misused.
  - Assures confidentiality and integrity of data
    - Protected communications aren't visible by others
    - Verifies data has been altered or corrupted
  - Provides Authentication
    - Verifies identity of participants
- The benefits of Cryptography are encryption. The data encryption provides security data at all times, integrity, privacy, compliance and protects the data across all devices.
- Hash Functions- Ensures the integrity of data. One-way functions-generate fixed-size representation of the input. Collision is a hash function generates the output for different inputs.
- Salt or Salting (cryptography) - Salting is random data that is used as an additional input to a one-way function that "hashes" data, a password or passphrase.  $\text{HASH}(\text{password} + \text{salt})$

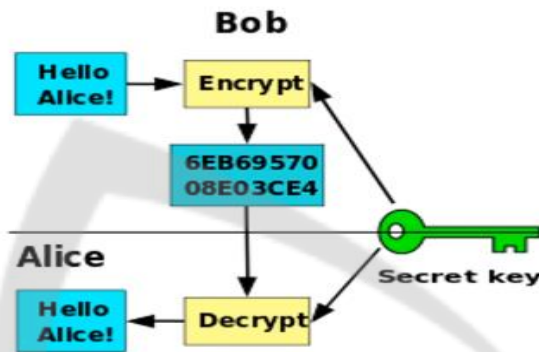
---

Brought to you by:

**CYBRARY** | FOR BUSINESS

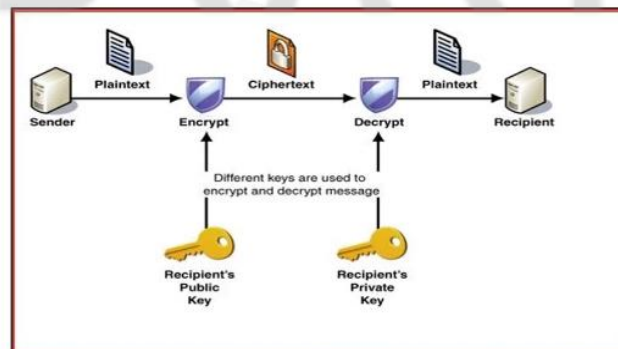
Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Symmetric Encryption



- Five Components of a Symmetric Encryption
  - Plaintext- refers to the original form not especially in any special format other than how it was written.
  - Encryption Algorithm- plaintext converted into an unreadable format.
  - Key- it is a decoder: the secret of the scrambled text cannot be read without the key.
  - Ciphertext- the text is scrambled and ready to be sent.
  - Decryption Algorithm- the secret key is applied to the ciphertext. It converts back to plaintext and reverses the encryption.

## Asymmetric Encryption



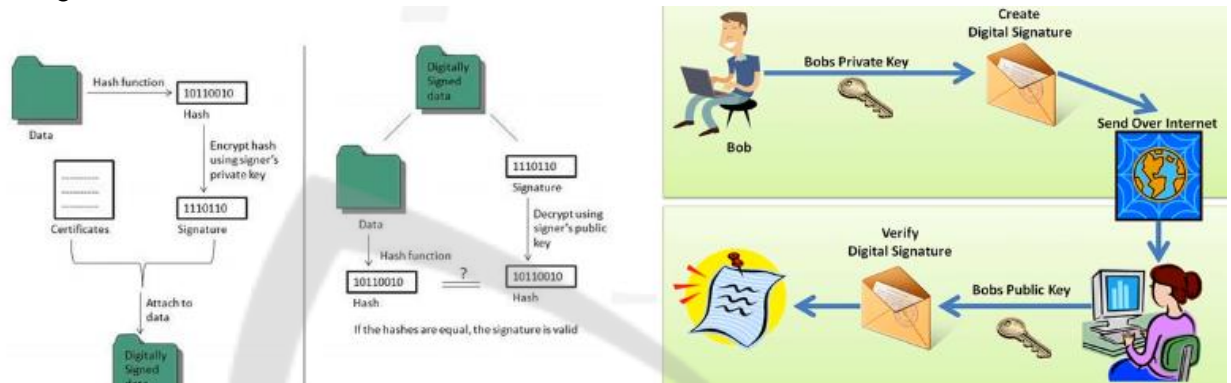
Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

# CYBRARY

- Digital Signatures provides authentication of a sender and integrity of a sender's message.



- Steganography is hiding one message inside of another. Steganography can be used to hide inside various forms of media like a photograph, an audio recording or video recording. It is mostly hidden in photographs such as JPEG or GIF.
- Non-repudiation is the assurance that the message cannot deny. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data.

## Lesson 4.3: Understand Requirements for Cryptography (11:05)

*Skills Learned From This Lesson: ISACA Model, Data Classifications, and End-User Privacy Training*

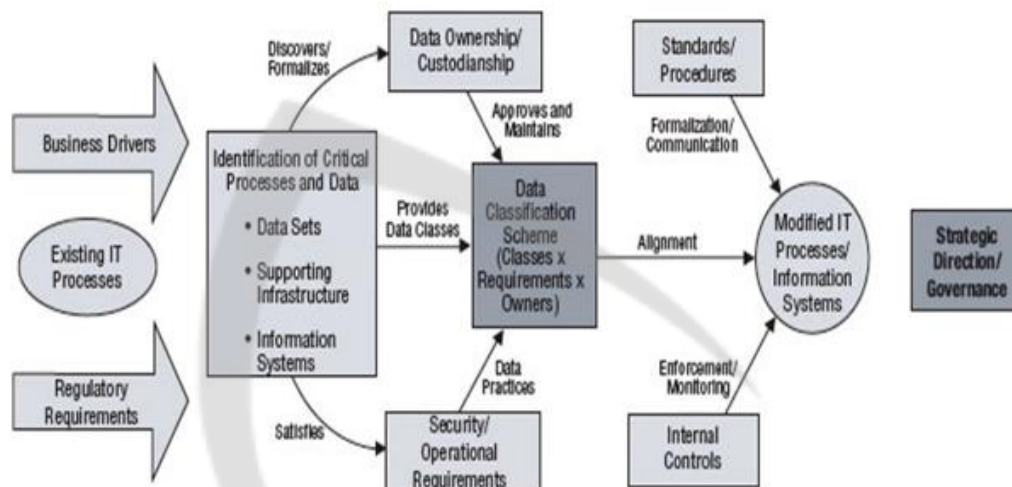
- ISACA Model for Business Data Classification is defined as a fundamental to asset management, risk assessment and the strategic use of security controls within the IT infrastructure of any organization. Without the understanding of different classes of data according to the assessed risk and value, it is impossible to allocate and maximize resources to ensure continuity of business operations.
- Cryptography encompasses the protection of information by altering it to ensure its integrity, confidentiality, and authenticity.

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## ISACA Model for Business Data Classification



- Policies, Standards, Guidelines, and Procedures- Policies are formal statements by upper management. Standards are mandatory actions or rules that give formal support to policies. Procedures are detailed step by step instructions to achieve the goals. Guidelines are recommendations to end-users when specific standards do not apply.
- Fundamental concepts and requirements for the use of cryptography include

Hashing	MD-5, SHA-512, HMAC
Salting	UNIX, internet security
Symmetric/Asymmetric encryption	Diffie-Hellman, RSA, ECC, Elgamal
Digital Signatures	RFC 2630
Non-repudiation	US Government CAC

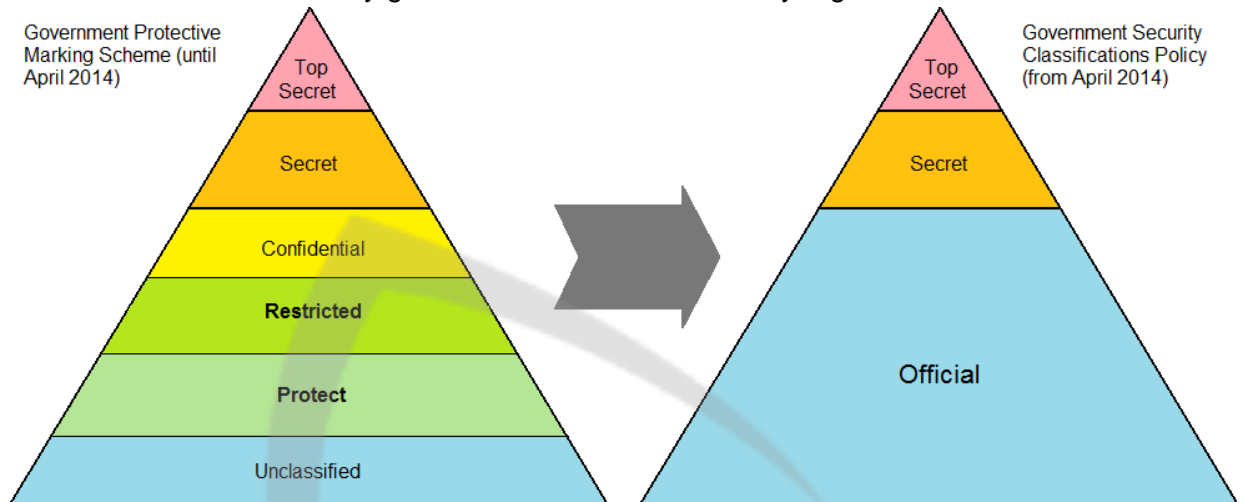
Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

# CYBRARY

- Data Classifications used by government civilian and military organizations.



- Data Classifications used by commercial organizations, from highest to lowest.

Information Classification	Examples
Sensitive	Passwords, encryption keys, payment card details
Confidential	Internal market research, audit reports
Private	Policies and procedures
Proprietary	Intellectual property
Public	Contact information

- End-User Privacy Training is security awareness training. It is the formal process for educating employees about computer security. A good security awareness program should educate employees about corporate policies and procedures for working with information technology (IT). The following topics related to information security and privacy restrictions:

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.



- The protection of classified or personally identifiable information maintained on computer systems.
- The authentication required to access classified or personally identifiable information.
- Responsibilities of third parties, including contractors, clients, and customers, with regard to classified or personally identifiable information.
- The consequences, including fines, sanctions, and penalties, of disclosing classified or personally identifiable information.

## Module 5: Integrated Host Security

### Lesson 5.2: Host Security Controls Part 1 (12:07)

*Skills Learned From This Lesson: Physical Security, Five-Step Process, and Patch Management*

- Securing control is defined as any device or process that is used to reduce risk. There are two levels of security controls:
  - Administrative controls- processes for developing and ensuring that policies and procedures are carried out.
  - Technical controls- controls that are carried out or managed by devices.
- External perimeter defenses are designed to restrict access to equipment areas physically.
- Internal physical access security recommends key management procedures, monitoring, and badge readers.
- A five-step process for protecting operating systems.
  - Develop the security policy
  - Perform host software baselining
  - Configure operating system security settings
  - Deploy and manage security settings
  - Implement patch management

---

*Brought to you by:*

**CYBRARY** | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

---

# CYBRARY

---

- Develop the security policy- a security policy is a document(s) that clearly defines an organization's defense mechanisms.
- Perform host software baselining
  - Baseline-the standard or check
  - Configuration settings that are used for each computer in the organization
- Configure operating system security and settings
  - Modern Oss has hundreds of different security settings that can be manipulated to conform to the baseline.
  - Typical configuration baseline would include:
    - Changing insecure default settings
    - Eliminating unnecessary software, services, and protocols
    - Enabling security features such as a firewall
- Deploy and Manage Security Settings
  - Tools to automate the process
    - Security template-collections of security configuration settings
    - Group policy- Windows feature providing centralized computer management; a single configuration may be deployed to many users
- Implement Patch Management
  - Operating systems have increased in size and complexity
  - New attack tools have made secure functions vulnerable
  - Security patch- software security update to repair discovered vulnerabilities
  - Hotfix- addresses specific customer situation
  - Service pack- accumulates security updates and additional features

## Lesson 5.3: Host Security Controls Part 2 (11:04)

*Skills Learned From This Lesson: Patch Updating, Best Practices and Options, and Various Definitions of Viruses*

- Patches can sometimes create new problems
  - The vendor should thoroughly test before deploying.
- Automated Patch Update Service

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

---

- Manage patches locally rather than rely on the vendor's online update service
- Advantages of automated patch update service
  - Administrators can force updates for "detection" only; allows them to see which computers will require the update without actually installing it.
  - Downloading patches from a local server instead of using the vendor's online update service can save bandwidth and time.
  - Specific types of updates that the organization does not test can be automatically installed.
  - Users cannot disable or circumvent updates.
- Install Only Necessary Software- The computer system must a designed goal. All installed software supports that goal.
- Some Oses are packaged better for only necessary software.
- Linux
  - Packaged in many small packages
  - Easier to select only what is needed and nothing more
- Secure necessary services: two choices
  - Disable
    - OS differences
    - System startup or server service.
  - Configure/constrain
    - TCP wrappers
    - Application-specific
    - May not be possible
- Secure weak default settings
  - Investigate and change weak default settings
  - Generally specific to OS and applications
  - Numerous guides are available to current best practices
- Security through design
  - OS hardening-tightening security during the design and coding of the OS

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- Trusted OS- an OS that has been designed through OS hardening
- Securing with Antimalware- third-party antimalware software packages can provide added security. Examples: Antivirus, Antispam, Popup Blockers, Antispyware, Host-based Firewalls
- Malicious Software (Malware) is designed to infiltrate or affect a computer system without the owner's informed consent. It is usually associated with various forms of worms, viruses, Trojan Horses, etc.
- A computer virus is a program that can copy itself and affect a computer system without the owner's informed consent

## Virus Symptoms

- Components of Windows or other programs no longer work.
  - Programs or files are suddenly missing.
  - Unusual messages or displays on your monitor.
  - Unusual sounds or music played at random times.
  - System has less available memory than it should.
  - Unknown programs or files have been created installed.
  - Your browser has unknown add-ins.
  - Files have become corrupted.
  - File size unexpectedly changes.
- Virus Hoax is a message warning the recipient of a non-existent computer virus threat, usually sent as a chain email that tells the recipient to forward it to everyone they know.
  - Trojan Horse is an executable program that appears as a desirable or useful program. It tricks the user into loading and executing the program.
  - Spyware is a type of malware that gets installed and collects personal information and browsing habits without the user's knowledge.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

---

- A rootkit is a software or hardware device designed to gain administrator-level control without being detected. Backdoor is a program that gives some remote and unauthorized control of a system.
- Antispam is services and solutions that focus on blocking and mitigating the effects of illegal emails or spam on email users. Mail servers can be configured to block unwanted emails and content filtering.
- Pop-up blockers are to prevent pop-up windows from appearing on websites. Usually, it can be turned on and off in the browser settings. Antispyware is software designed to detect and remove unwanted spyware programs.
- Host-Based Firewalls- It is firewall software that runs on an individual computer or device connected to a network, also called a personal firewall. Both Linux and Windows use host-based firewalls. They have no part of your enterprise server's security programs. It is too much configuration and usually, you configure to user-specific.

## Lesson 5.4: Application Development Security (06:30)

*Skills Learned From This Lesson: Application Security, Application Coding, and Error Handling*

- Application security is about protecting the applications by finding, fixing and preventing security vulnerabilities. It can be done during application development. It will also be followed through the life cycle of the software by hotfixes, applications hardening, and patch management. This applies to operating systems as well.
- Application development security must be considered through all phases of the development cycle. Application configuration baselines:
  - Standard environments settings can establish a secure baseline
  - Includes each development system, build system, and test system
  - Must include system and network configurations
- Securing coding concepts increase applications' consistency, reliability, and security. It allows developers to quickly understand and work with code that has been developed by other members. Example of a coding standard:
  - A wrapper function is substituted as a regular function in testing to write error-checking routines for preexisting systems functions.

---

*Brought to you by:*

**CYBRARY** | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Errors and Exception Handling:
  - Errors- faults that occur while an application is running
  - Response to the user should be based on the error
  - The application should be coded so that each error is “caught” and effectively handled.
  - Improper error handling in an application can lead to application failure.
- Indication of potential error-handling issues:
  - Failure to check return codes or handle exceptions
  - Improper checking of exceptions or return codes
  - Handling of all codes or exceptions in the same manner
  - Error information that divulges potentially sensitive data
- Input Validation is a specific type of error handling ids verifying responses that the user makes to the application: Causes improper verification of XSS, SQL, or XML injections.

## Lesson 5.5: How to Secure Data (05:34)

*Skills Learned From This Lesson: Big Data, DLP systems, DLP sensors and securing data*

- Big Data refers to a collection of data sets so large and complex that it becomes difficult to process using traditional data processing apps.
- Data Loss Prevention (DLP) - It is a set of tools and processes used to recognize and identify sensitive *data* so *it* is not lost, misused, or accessed by unauthorized users making sure it is protected.
- DLP systems use content inspection.
  - A security analysis of the transaction within its approved context
  - Looks at the security level of data, who is requesting it, where the data is stored, when it was requested, and where it is going.
- DLP systems can also use indexing matching.
  - Documents that have been identified as needing protection are analyzed by DLP and complex computation is conducted based on the analysis.

---

*Brought to you by:*

**CYBRARY** | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

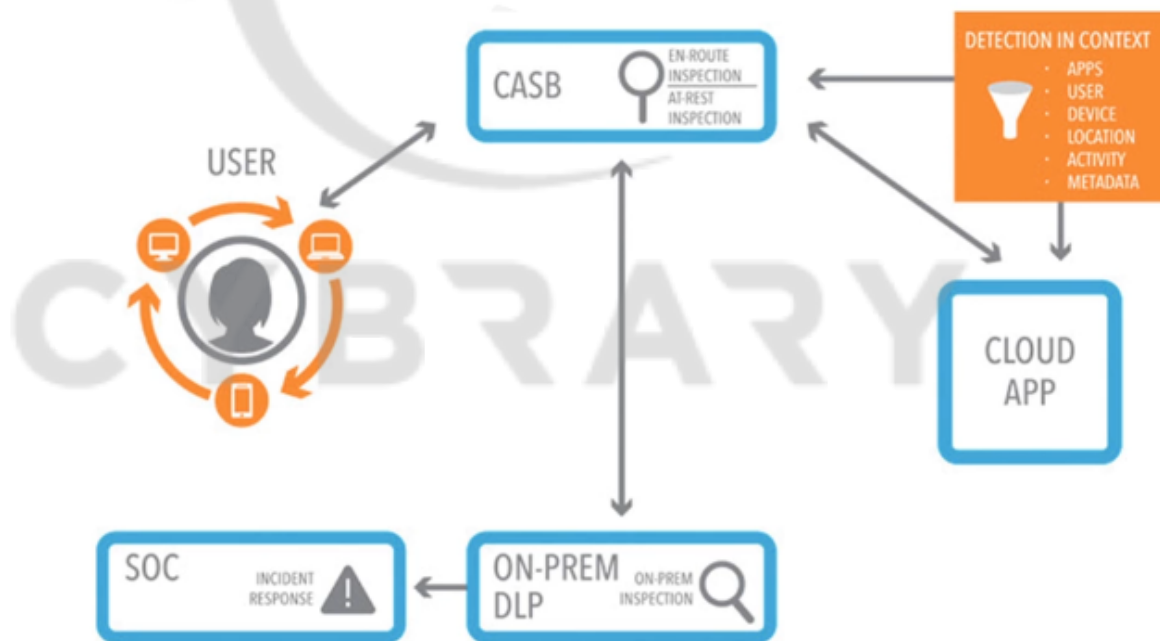
---

# CYBRARY

---

- DLP examines data as it resides in any three states:
  - Data in use (for example: creating a report from a computer)
  - Data in-transit (data being transmitted)
  - Data at rest (data that is stored on electronic media)
- Three types of DLP sensors:
  - DLP network sensors- installed on the perimeter of the network to protect data-in-transit by monitoring all network traffic.
  - DLP storage sensors- designed to protect data-at-rest
  - DLP agent sensors- installed on each host device and protect data in-use
- When a policy violation is detected by the DLP agent, it is reported back to the DLP server. Different actions can then be taken.

## Securing Data



---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

---

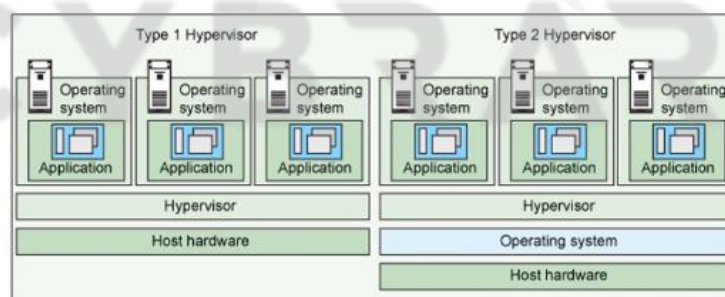
## Lesson 5.6: Operate and Secure Virtual Environments (06:59)

*Skills Learned From This Lesson: Software Defined Networking, Virtualization, Hypervisor, Virtual Appliance, and Shared Storage*

- Software-Defined Networking (SDN) is a centralized network architecture approach that enables the network to be intelligently and controlled, or ‘programmed,’ using software applications.
- Virtualization means is creating more logical IT resources, called hypervisor to emulate the underlying hardware and manage resources for each virtual system. Virtualization is changing the mindset from physical to logical.
- The hypervisor is what controls and allocates what portion of hardware resources each operating system should get, in order every one of them to get what they need without disrupting other virtual environments.

## Two types of hypervisors

- Type 1 hypervisor: hypervisors run directly on the system hardware – A “bare metal” embedded hypervisor,
- Type 2 hypervisor: hypervisors run on a host operating system that provides virtualization services, such as I/O device support and memory management.



- A virtual appliance is a software application residing and operating in a preconfigured virtual environment or platform. It can be accessed remotely by users and does not require locally-installed hardware.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.



---

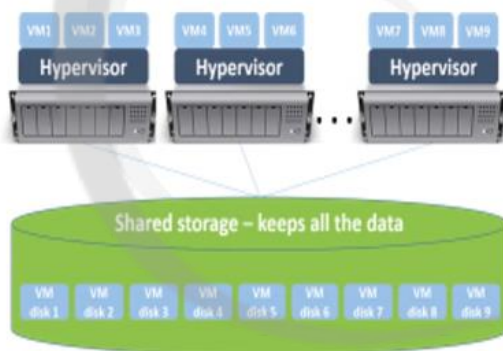
# CYBRARY

---

- IT continuity (information technology continuity) is a holistic approach to managing technology systems in the event of a major disruption.
- Resilience refers to a network or system's ability to withstand the slings or arrows of life and operations, from a human error to migration failure to natural disaster.

## Shared Storage

- Shared storage is “centralizing” data in one “place” however it is more than just that.
- In today's business environment, it is imperative that data be accessible on a 24/7 basis and not be subjected to hardware issues.



### Lesson 5.7: Operate and Configure Cloud Security (13:40)

*Skills Learned From This Lesson: Cloud Computing, Four Cloud Models, Data Storage, and Transmission, Third Party/Outsourcing Requirements, and Security Interaction Model*

- Cloud Computing is a network of remote servers that are scalable storage and applications accessed over the internet.
- The Four Cloud Models of Cloud Computing:
  - Software as a Service (SaaS) - Applications run on the vendor's cloud, which they, control and maintain.
  - Platform as a Service (PaaS) - A vendor provides the business with a platform upon which can be developed and run applications.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- Infrastructure as a Service (IaaS) - It allows your business to have complete, scalable control over the management and customization of your infrastructure while the vendor just provides the space and access over the internet.
- Networking as a Service (NaaS) – It is the sale of *network services* from third parties to customers that don't want to build their own *networking* infrastructure.
- Legal and privacy concerns challenge and complexity of complying with legislation, regulations, and laws issued by countries worldwide will become an ever-increasing challenge for cloud providers as well as cloud users.
- Surveillance is an ongoing close observation and collection of data or evidence, for a specified purpose or confined to a narrow sector. In comparison, environmental scanning broad and includes all associated external factors.
- Data ownership is the act of having legal rights and complete control over a single piece or sets data elements.
- Jurisdiction is the power or right of a legal or political agency to exercise its authority over a person, subject matter, or territory.

## Data storage and transmission

- ▷ Archiving-Data archiving is the process of moving data that is no longer actively used to a separate storage device for long-term retention. Archive data consists of older data that is still important to the organization and may be needed for future reference, as well as data that must be retained for regulatory compliance.
- ▷ Recovery-Data recovery is the process of restoring data that has been lost, accidentally deleted, corrupted or made inaccessible.
- ▷ Resilience-In computer networking: resilience is the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.” Threats and challenges for services can range from simple misconfiguration over large scale natural disasters to targeted attacks.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Third-party/outsourcing requirements

- ▷ A good SLA is important because it sets boundaries and expectations for the following aspects of data center service provisioning.
- ▷ An SLA drives internal processes by setting a clear, measurable standard of performance.
- ▷ Data portability refers to the ability to move, copy or transfer data easily from one database, storage or IT environment to another.
- ▷ Data destruction is the process of destroying data stored on tapes, hard disks and other forms of electronic media so that it is completely unreadable and cannot be accessed or used for unauthorized purposes.
- ▷ Auditing is the examination and evaluation of an organization's information technology infrastructure, policies and operations.

## Security Interaction Model



Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the *fastest growing catalog* in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Lesson 5.8: Mobile Device Security (12:07)

*Skills Learned From This Lesson: Mobile Device Defined, Steps to Secure Mobile Devices, and Mobile Device Management*

- A mobile device is a portable, wireless computing device that is small enough to be held in the hand. Mobile device security is security measures designed to protect the sensitive information stored on and transmitted on a mobile device.
- Mobile device security risks:
  - Limited physical security can be stolen.
  - Connecting to public networks
  - Location tracking
  - Installing unsecured applications
  - Accessing untrusted content
  - Bring your own device (BYOD) risks that can be shared with unauthorized users, termination of employment, and different limitations on various devices.
- Steps to securing mobile devices:
  - Initial setup of device-disable unused features, enable lock screen, set of passcodes, encrypt device and control access.
  - It's ongoing management of mobile device management(MDM)-
    - Apply application whitelisting- ensures only pre-approved applications are being used.
    - Geo-fencing- uses the GPS to define the geographical boundaries where the app can be used.
    - Credential management- stores authentication information.
  - Dealing with theft or loss of devices- always be aware of the location of the device, report it stolen as soon as you realize it and remote wipe it if stolen.
  - Bring your own device (BYOD) security- write and enforce defined policies include the same policies you would for a company device.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

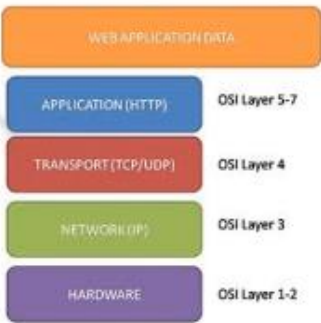
Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Module 6: Secure Development

Lesson 6.2: Software Responsibilities Part 1 (06:28)

*Skills Learned From This Lesson: Application Security Fundamentals, Escalation of Privileges, and Software Vulnerabilities*

### Application Security Fundamentals

- Application security includes measures taken throughout an application's life-cycle to prevent exceptions in the security policy of an application or the underlying system (vulnerabilities) through flaws in the design, development, deployment, upgrade, or maintenance of the application.\*
  - The primary focus is on Layer 7 of the OSI Model
  - AppSec should be part of an organization's or vendor's Software (or System) Development Life-Cycle (SDLC)
  - A key component of application security should be for developers and their managers to be aware of basic AppSec requirements, common threats and effective countermeasures
  - AppSec knowledge and maturity is significantly lower today than traditional network security
- 
- A software vulnerability is a glitch, flaw, or weakness present in the software or the operating system. Software vulnerabilities are explained by three factors:
    - Existence- the existence of a vulnerability in the software
    - Access- the possibility that hackers gain access to the vulnerability
    - Exploit- the capability of the hacker to take advantage of that vulnerability via tools and techniques
  - A vulnerability assessment is a process of identifying, quantifying and prioritizing the vulnerabilities in a system. The process is intended to identify threats and the risks they pose typically involves the use of automated tools, etc.

Brought to you by:

**CYBRARY** | FOR BUSINESS

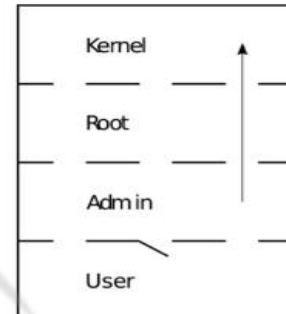
Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.



## Escalation of Privilege

- Privilege escalation occurs when code runs with higher privileges than that of the user who executed it. Privilege escalation techniques include:

-----Vertical privilege escalation  
-----Horizontal privilege escalation



- Two types of privilege escalation:
  - Vertical privilege escalation- is a lower privilege user or application accesses functions or content reserved for higher privilege users or applications.
  - Horizontal privilege escalation- a normal user accesses functions or content reserved for another normal user.

### Lesson 6.3: Software Responsibilities Part 2 (10:59)

*Skills Learned From This Lesson: Skill, Skill, Skill*

- Top 10 software vulnerability list for 2019
  - 1. Buffer Overflow
  - 2. Directory traversal
  - 3. Failure to protect sensitive data
  - 4. Issues with libraries, components, and dependencies
  - 5. Issues with web services and APIs
  - 6. Issues with logging ( too little/ too much)
  - 7. Cross-site scripting
  - 8. Missing or broken authentication
  - 9. Missing or broken authorization (access control)
  - 10. SQL injection

*Brought to you by:*

**CYBRARY** | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

---

# CYBRARY

---

- Buffer Overflow occurs when more data are written to a buffer than it can hold. It happens when there is improper validation no bounds prior to the data being written. It is considered a bug or weakness in the software. The overflow data might contain executable code that allows the attackers to run bigger and more sophisticated programs or grant themselves access to the system.
- Directory Traversal is a security exploit within HTTP that enables an individual to access restricted files or directories and execute commands that are external to the Web server's root directory. It generally happens as a result of a lack of or insufficient validation within the code of applications hosted/executed on the Web server.
- Failure to protect sensitive data can be caused by the loss of connectivity threatens customers temporarily. Loss of sensitive data threatens customers for the rest of their lives and can have severe consequences for the business.
- Issues with libraries, components, and dependencies have code containing some existing code, whether in the form of self-contained modules or snippets "borrowed" from other codebases. The convenience of code reuse comes with threats:
  - New vulnerabilities are discovered all the time.
  - Malicious actors can take over trusted components.
- Code Reuse is the use of a single piece code several times, whether in an application or reused and evolves from one version to the next.
- Resource Exhaustion is a denial of service (DoS) technique that occurs when the resources necessary to perform an action are completely consumed. They are computer security exploits that crash, hang, or otherwise interfere with the program or system.
- Issues with web services and APIs aren't kept up and threat actors can sometimes access sensitive data directly via unsecure services and APIs.
- Issues with logging (too little/too much) by doing so can help you detect an attack and determine its scope and potential damage after the fact.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

---

- Cross-site scripting is a type of security vulnerability found in web applications. It is sent a script that activates when read by an unsuspecting user's browser or the application isn't protected against it.
- OS fingerprinting is the process of learning what operating system is running on a particular device. OS fingerprinting techniques:
  - Passive OS fingerprinting is the process of analyzing packets from a host on a network. A fingerprinter acts as a sniffer and doesn't put any traffic on a network.
  - Active OS fingerprinting is the process of transmitting packets to a remote host and analyzing corresponding replies.
- Cross-site request forgery (CSRF), also known as XSRF, Sea Surf or Session Riding, is an attack vector that tricks a web browser into executing an unwanted action in an application to which a user is logged in.
- Missing or broken authentication is the process of verifying the identity of a person or device. There are three common factors used for authentication: something you know (such as a password), something you have (such as a smart card), and something you are (such as a fingerprint or another biometric method).
- Missing or broken authorization (access control) – the authorization is a security mechanism used to determine user/client privileges or access levels related to system resources, including computer programs, files, services, data, and application features. Access control is a way of limiting access to a system or to physical or virtual resources.
- SQL Injections- It is a computer attack in which malicious code is embedded in a poorly-designed application and passed to the backend database. The malicious data then produces database query results or actions that should never have been executed.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.



## What Goes Into An Application Test?

- Application security goes well beyond simply running a scanning tool. For critical or high value applications, or those that process sensitive data, thorough testing may actually include a combination of several methods.

Unauthenticated Automated Scan	Authenticated Automated Scan	Automated Binary Analysis
Blind Penetration Testing	Manual Source Code Review	Manual Binary Analysis
Informed Manual Testing	Automated Source Code Scanning	

## Tools and Resources

- Open Software Assurance Maturity Model (OpenSAMM) – A freely available open source framework that organizations can use to build and assess their software security programs [www.opensamm.org](http://www.opensamm.org)
- The Open Web Application Security Project (OWASP) – Worldwide not-for-profit organization focused on improving the security of software. Source of valuable free resources [www.owasp.org](http://www.owasp.org)
- Open Source or Low Cost Application Security Scanners – OWASP Zed Attack Proxy (ZAP), w3af, Mavrituna Netsparker, Websecurify, Wapiti, N- Stalker, SkipFish, ScrawlR, Acunetix, and many more to do basic discovery work

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

---

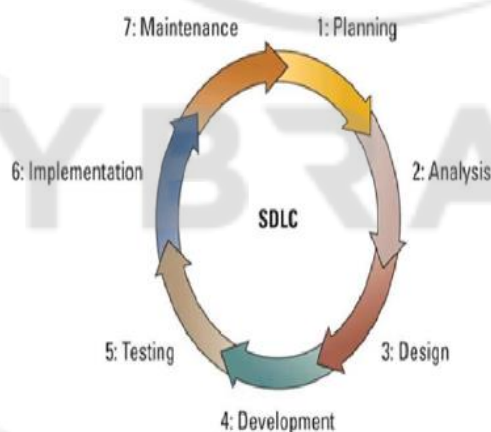
## Lesson 6.4: Software Development Part 1 (05:05)

*Skills Learned From This Lesson: Software Security, Software Assurance, and Secure DevOps*

- Software Security is to protect software in the development process and ongoing process against malicious attack and other hacker risks so that the software continues to function correctly under such risks or threats.
- Software Assurance is defined as “the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle, and that the software functions in an intended manner.
- Secure DevOps is the process of integrating secure development best practices and methodologies into the development and deployment process possible. It also includes security checks and reviews through the process.

## Lesson 6.5: Software Development Part 2 (05:24)

*Skills Learned From This Lesson: SDLC, Six Distinct Phases, Six Distinct Phases Defined, and Application Security*



---

Brought to you by:

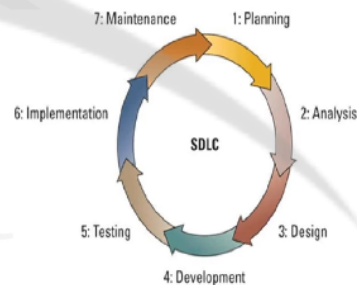
**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- Systems Development Life Cycle (SDLC) – all systems have a life cycle or a series of stages they naturally undergo. The number and name of the stages vary, but the primary stages are conception, development, maturity, and decline. It actually refers to the development stage of the system's life cycle.

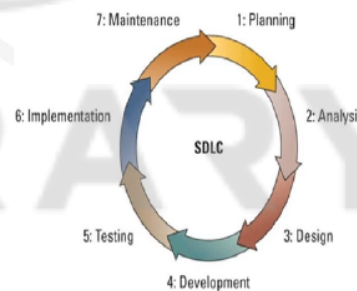
## Systems Development Life Cycle

- The 6 distinct phases:
  - Project Identification and Selection
  - Project Initiation and Planning
  - Analysis
  - Design
  - Implementation
  - Maintenance



## Phases of the Systems Development Life Cycle

1. Project Identification and Selection
  - Two Main Activities
    - Identification of need
    - Prioritization and translation of need into a development schedule
  - Helps organization to determine whether or not resources should be dedicated to a project.
2. Project Initiation and Planning
  - Two Activities
    - Formal preliminary investigation of the problem at hand
    - Presentation of reasons why system should or should not be developed by the organization



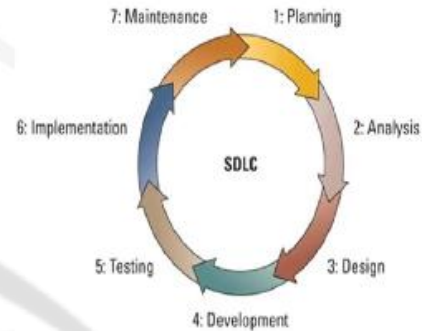
Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

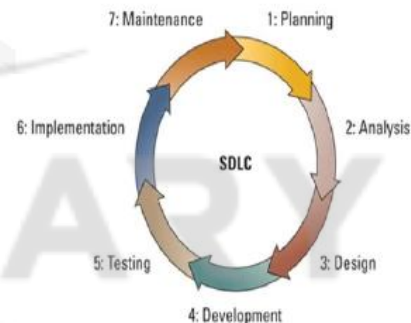
## Systems Development Life Cycle

- Analysis
  - Study of current procedures and information systems
    - Determine requirements
      - Study current system
      - Structure requirements and eliminate redundancies
    - Generate alternative designs
    - Compare alternatives
    - Recommend best alternative



## Systems Development Life Cycle

- Design
  - Logical Design
    - Concentrates on business aspects of the system
  - Physical Design
    - Technical specifications
- Implementation
  - Implementation
    - Hardware and software installation
    - Programming
    - User Training
    - Documentation



Brought to you by:

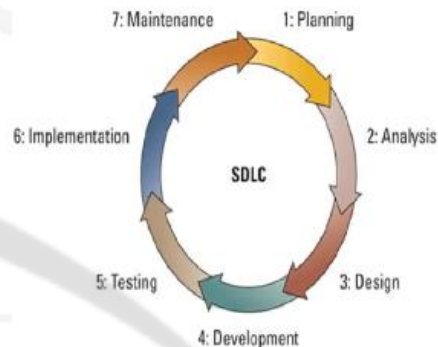
**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Systems Development Life Cycle

- Maintenance
  - System changed to reflect changing conditions
  - System obsolescence

A good way to learn the stages of the SDLC is to create **deliverables** (output) of each stage in the process.



- Alternative Approaches
  - Prototyping
    - Building a scale-down working version of the system. The advantages are users are involved and capture in concrete form.
    - Rapid Application Development (RAD) utilizes prototyping to delay producing system design until requirements are clear.

## What Goes Into An Application Test?

- Application security goes well beyond simply running a scanning tool. For critical or high value applications, or those that process sensitive data, thorough testing may actually include a combination of several methods.

Unauthenticated  
Automated Scan

Authenticated  
Automated Scan

Automated  
Binary Analysis

Blind Penetration  
Testing

Manual Source  
Code Review

Manual Binary  
Analysis

Informed Manual  
Testing

Automated  
Source Code  
Scanning

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

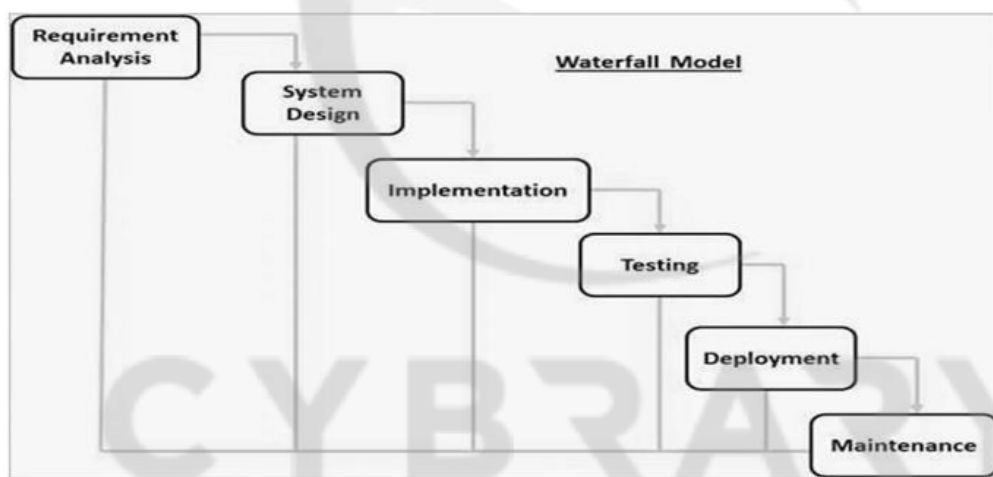


## Lesson 6.6: Software Development Part 3 (10:11)

*Skills Learned From This Lesson: SDLC Models, SDLC Models Defined, and Secure Coding Defined*

- SDLC Models:
  - Waterfall Model
  - Iterative Model
  - Spiral Model
  - V-Model
  - Big Bang Model

### Waterfall Model - Design



- Waterfall Model Advantages:
  - Simple and easy to understand and use.
  - Phases are processed and completed one at a time.
  - Works well for smaller projects where requirements are very well understood.
  - Clearly defined stages.
  - Well understood milestones.
  - Easy to arrange tasks.
  - The process and results are well documented.

---

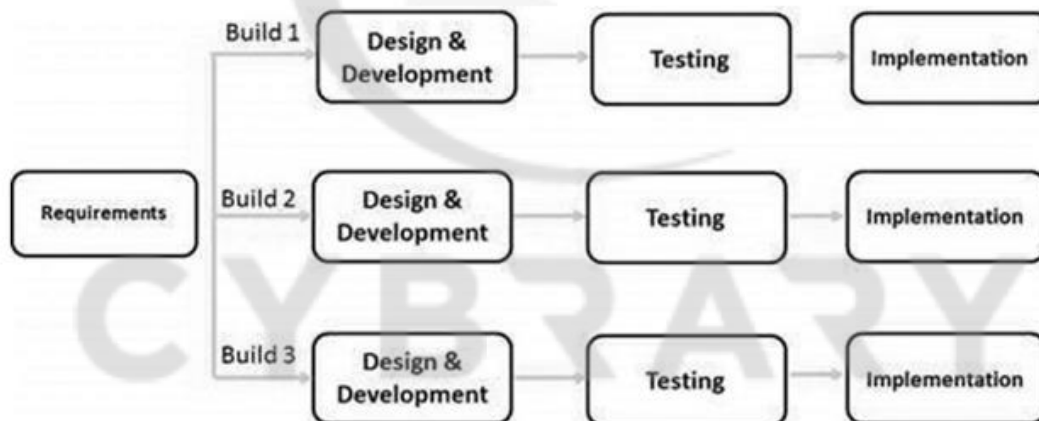
*Brought to you by:*

**CYBRARY** | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Waterfall Model Disadvantages:
  - No working software is produced until late during the life cycle.
  - High amounts of risk and uncertainty.
  - Poor model of risk and uncertainty.
  - Not a good model for complex and object-oriented projects.
  - Not suitable for the projects where requirements are at a moderate to high risk of changing. So, risk and uncertainty are high with this process model.
  - It is difficult to measure progress within stages.
  - It cannot accommodate changing requirements.
  - Adjusting scope during the life cycle can end a project.
  - Integration is done as a “big-bang”. At the very end, this doesn’t allow identifying any technological or business bottleneck or challenges early.

## Iterative Model



- Iterative Model- Advantage
  - Some working functionality can be developed quickly and early in the life cycle.
  - Results are obtained early and periodically.
  - Progress can be measured.
  - Less costly to change the scope/requirements.
  - Testing and debugging during smaller iteration is easy.

---

Brought to you by:

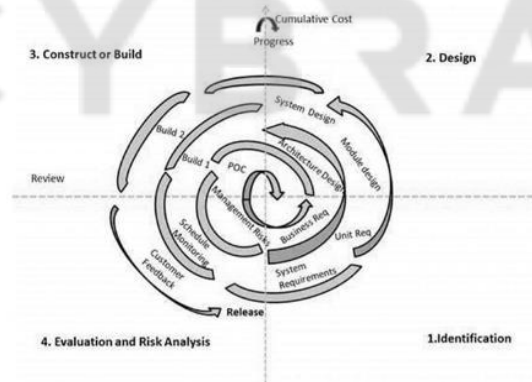
**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

# CYBRARY

- Risks are identified and resolved during iteration, and each of the iterations is an easily managed milestone.
- Easier to manage risk-High risk part is done first.
- With every increment, the operational product is delivered.
- Issues, challenges, and risk identified from each increment can be utilized/applied to the next increment.
- Risk analysis is better.
- Iterative Model- Disadvantage
  - More resources may be required.
  - Although the cost of change is lesser, it is not very suitable for changing requirements.
  - A system architecture or design issues may arise because not all requirements are gathered at the beginning of the entire life cycle.
  - Defining increments may require a definition of the complete system.
  - Not suitable for smaller projects.
  - Management complexity is more.
  - The end of the project may not be known which risk is.
  - Highly skilled resources are retired for risk analysis.
  - Project progress is highly dependent upon the risk analysis phase.

## Spiral model



Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.



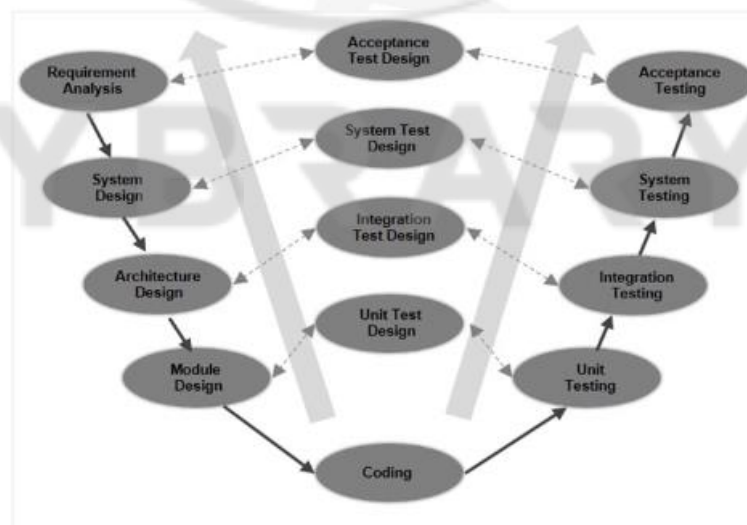
---

# CYBRARY

---

- Spiral SDLC Model -Advantage
  - Changing requirements can be accommodated.
  - It allows extensive use of prototypes.
  - Requirements can be captured more accurately.
  - Users see the system early.
  - Development can be divided into smaller parts and the risky parts can be developed earlier which helps in better risk management.
- Spiral SDLC Model- Disadvantage
  - Management is more complex.
  - The end of the project may not be known early.
  - Not suitable for small or low-risk projects and could be expensive for small projects.
  - The process is complex.
  - Spiral may go on indefinitely.
  - Large number of intermediate stages requires excessive documentation.

## V-model



---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- V- Model- Advantage
  - This is a highly-disciplined model and phases are completed one at a time.
  - Works well for smaller projects where requirements are very well understood.
  - Simple and easy to understand and use.
  - Easy to manage due to the rigidity of the model. Each phase has specific deliverables and a review process.
- V- Model- Disadvantage
  - High risk and uncertainty.
  - Not a good model for complex and object-oriented projects.
  - Poor model for long and ongoing projects.
  - Not suitable for the projects where requirements are at a moderate to high risk of changing.
  - Once an application is in the testing stage, it is difficult to go back and change functionality.
  - No working software is produced until late during the life cycle.
- Big Bang Model
  - The Big Bang Model is an SDLC model where we do not follow any specific process. The development just starts with the required money and efforts as the input, and the output is the software developed which may or may not be as per customer requirement.
  - Usually, this model is followed for small projects where the developments teams are very small.
- Big Bang Model- Advantage
  - This is a very simple model.
  - Little or no planning required.
  - Easy to manage.
  - Very few resources required.
  - Gives flexibility to developers
  - It is a good learning aid for newcomers or students.
- Big Bang Model- Disadvantage
  - Very high risk and uncertainty.
  - Not a good model for complex and object-oriented projects.

- Poor model for long and ongoing projects.
- It can turn out to be expensive if requirements are misunderstood.
- Secure coding is the practice of writing software that's protected from vulnerabilities. It is important for all software no matter what platforms it runs on. You should become familiar with the techniques and tools to support this practice.
- Risk of Insecure Software
  - Denial of service to a single user.
  - Compromised secrets.
  - Loss of service.
  - Damage to the systems of thousands of users.
  - Loss of life.

## Lesson 6.7: Software Development Part 4 (05:21)

*Skills Learned From This Lesson: Secure Coding Practices, Different Aspects of Fuzz Testing, and Session Management*

- Secure Coding Practices
  - 1. Don't leave security until the end of development.
  - 2. Consider the Motive for Attack.
  - 3. No One is Safe.
- Secure coding standards are the rules and guidelines used to prevent security vulnerabilities. Used effectively, secure coding standards prevent, detect, and eliminate errors that could compromise software security.
- Session Management attacks occur when an attacker breaks into the web application's session management mechanism to bypass the authentication controls and spoof the valid user. Two techniques are typically used:
  - Session token prediction
  - Session token sniffing and tampering
- Fuzz Testing is a type of testing where automated or semi-automated testing techniques are used to discover coding errors and security loopholes in software,

---

*Brought to you by:*

**CYBRARY** | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

operating systems, or networks by inputting invalid or random data called FUZZ to the system

- The system is monitored for various exceptions, such as crashing down the system or failing built-in code, etc.
- How to do Fuzz Testing
  - Step 1) Identify the target system
  - Step 2) Identify inputs
  - Step 3) Generate fuzzed data
  - Step 4) Execute the test using fuzzy data
  - Step 5) Monitor system behavior
  - Step 6) Log defects
- Example of Fuzzers
  - Mutation-Based Fuzzers
  - Generation-Based Fuzzers
- Fuzz Testing Summary- fuzz testing shows the presence of bugs in an application. It cannot guarantee the detection of bugs completely in an application. But by using the Fuzz technique, it ensures that the application is robust and secure, as this technique helps to expose most common vulnerabilities.

## Module 7: Network Security Architecture

Lesson 7.2: Network Security Devices Part 1 (09:57)

*Skills Learned From This Lesson: OSI Model, Load Balancing, and Firewalls*

- Security through network devices can be achieved through layered network security by using networking devices or hardware designed for security:
  - Layered security- A defense that uses multiple types of security devices to protect a network. It is also called defense in depth.
  - A network with layered security will make it more difficult for an attacker. He must have all the tools, knowledge, and skills to break through the various layers.

---

*Brought to you by:*

**CYBRARY** | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

---

# CYBRARY

---

- Standard Networking Devices- Network devices can be classified based on their function in the OSI model. Standards released in 1978, revised in 1983, still used today. It also illustrates how to prepare network data for delivery and how the data is handled once it is received.
- OSI model breaks networking steps into seven layers.

Layer	Function	Example
<b>Application (7)</b>	Services that are used with end user applications	SMTP,
<b>Presentation (6)</b>	Formats the data so that it can be viewed by the user Encrypt and decrypt	JPG, GIF, HTTPS, SSL, TLS
<b>Session (5)</b>	Establishes/ends connections between two hosts	NetBIOS, PPTP
<b>Transport (4)</b>	Responsible for the transport protocol and error handling	TCP, UDP
<b>Network (3)</b>	Reads the IP address from the packet.	Routers, Layer 3 Switches
<b>Data Link (2)</b>	Reads the MAC address from the data packet	Switches
<b>Physical (1)</b>	Send data on to the physical wire.	Hubs, NICS, Cable

- Each layer has different networking tasks.
  - Each layer cooperates with adjacent layers.
  - Standards network devices can be classified by the OSI layer at which they function.
- Network administrators should monitor network traffic. Traffic monitoring methods:

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- Port Mirroring- It allows administrators to configure the switch to copy traffic that occurs on some or all ports to a designed monitoring port on the switch.
- Network Tap (test access point) - Separate device installed between two network devices.
- Load Balancers- Help evenly distributes work across a network and allocates requests among multiple devices.
- Advantages of load-balancing technology:
  - Reduces the probability of overloading a single server.
  - Optimizes bandwidth of networking computers.
  - Reduces network downtime.
- Load balancing is achieved through software or hardware devices. They are grouped into two categories:
  - Layer 4 load balancers- act upon data found in Network and Transport layer protocols.
  - Layer 7 load balancers-distribute requests based on data found in Application layer protocols.
- Security advantages of loading balancing:
  - Can detect stop attacks directed at a server or application.
  - It can detect and prevent denial-of-service (Dos) and protocol attacks.
  - Some can deny the attacker's information about the network.
    - Hide HTTP error pages.
    - Remove server identification headers from HTTP responses.
- Proxies- There are several types of proxies used in computer networking.
  - Proxy server- A computer or application program that intercepts users' requests from the internal networks and processes that request on behalf of the user.
  - Application-aware proxy- a special proxy server that “knows” the application protocols that it supports.
- Advantages of proxy servers:
  - Increased speed
  - Reduced costs

- Improved management
  - Stronger security
- A reverse proxy does not serve clients and routes incoming requests to the correct server.
- Network Firewalls:
  - It can be software or hardware-based.
  - Both types inspect packets and either accept or deny entry.
  - Hardware firewalls are usually located outside the network security perimeter.
- Methods of firewall packet filtering:
  - Stateless packet filtering- Inspects incoming packet and permits or denies based on the condition set by administrators
  - Stateful packet filtering- Keeps a record of the state of a connection and makes a decision based on the conditions and connections.
- Firewall actions on a packet
  - Allow (let packet pass-through)
  - Drop ( prevent the packet from passing into the network and send no response to sender)
  - Reject (prevent the packet from passing into the network but send a message to the sender)
- Rule-based Firewalls
  - Use a set of individual instructions to control actions, called firewall rules.
  - Each rule is a separate instruction processed in sequence telling firewall what action to take.

## Lesson 7.3: Network Security Devices Part 2 (10:45)

*Skills Learned From This Lesson: Various Firewalls, Spam Filters, VPNs, IDS, NIDS, and HIDS*

- Application-Aware Firewalls- Sometimes called Next-Generation Firewall (NGFW). Operates at a higher level by identifying an application that sends packets through the firewall and makes decisions about what action to take.

---

*Brought to you by:*

**CYBRARY** | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Web Applications Firewalls- Special type of application-aware firewall that looks deeply into packets that carry HTTP traffic. Can block specific sites or specific types of HTTP traffic.
- Spam Filters- It is a program that detects unsolicited and unwanted email and prevents messages from getting to the end user email.
- Two Types of Email Protocols:
  - Simple Mail Transfer Protocol (SMTP) - Handles outgoing mail.
  - Post Office Protocol (POP) - Handles incoming mail.
- Spam filters installed on the SMTP server is configured to listen on port 25. It passes non-spam email to SMTP server listening on another port. This method prevents the SMTP server from notifying spammer of failed message delivery.
- Spam filters installed on the POP3 server. All spam must first pass through an SMTP server and be delivered to the user's mailbox. It can result in increased costs. Third-party entity contract to filter spam. All emails directed to third-party remote spam filters and all e-mail is cleansed before redirected to the organization.
- Virtual Private Network (VPN) – It enables authorized users to use an unsecured public network as if it is a secure private network. All data transmitted between the remote devices and networks is encrypted. There are types of VPNs:
  - Remote-access VPN –a user to LAN connection
  - Site –to-site multiple sites can connect to other sites over the internet.
- Endpoints
  - The end of the tunnel between VPN devices
  - Used in communicating VPN transmissions
  - Maybe software on a local computer, a VPN concentrator (hardware device), or integrated into another networking device.
- VPN concentrator- a dedicated hardware device that aggregates hundreds or thousands of VPN connections. Tunneling protocols enclose a packet within another packet and are used for VPN transmissions.



- IPsec has two “subprotocols” that are used in VPN:
  - Encapsulated Security Payload (ESP)
  - Authentication Header
- A remote-access VPN generally uses either IPsec or the Layer 2 Tunneling Protocol (L2TP)
- Internet Content Filters- It a program designed to limit web material that can be viewed as what a parent would do to block certain sites (unapproved sites) for children.
- Web Security Gateways- Can block malicious content in real-time. Blocks content through application-level filtering like adware, spyware, cookies, etc.
- An intrusion detection system (IDS) – It detects attacks as they occur. It can be software or hardware designed to automatically alerts when someone or something is trying to compromise *information* systems through unauthorized activities.
- Monitoring Methodologies: There are different methodologies:
  - Anomaly-based monitoring that compares current detected behavior with baseline.
  - Signature-based monitoring looks for well-known attack signatures patterns.
  - Behavior-based monitoring detects abnormal actions by processes or programs. Alerts user who decides whether to allow or block activity.
  - Heuristic monitoring uses experience-based techniques.
- Types of IDS – two basic types of IDS exist. Host intrusion detection systems (HIDS):
  - A software-based application that can detect an attack as it occurs
  - Installed on each system needing protection
  - Monitors:
    - System calls and files system access.
    - Can recognize unauthorized Registry modification.
    - Host input and output communications.
      - Detects anomalous activity.
- Disadvantages of HIDS
  - It cannot monitor network traffic that does not reach the local system.

- All log data is stored locally.
- Resource-intensive and can slow system.
- Network Intrusion Detection System (NIDS) watches for attacks on the network. NIDS sensors installed on firewalls and routers:
  - Gather information and report back to the central device.
- Passive NIDS will sound an alarm.
- Intrusion Prevention System (IPS)
  - Monitors network traffic to immediately block a malicious attack.
  - Similar to NIDS
  - NIPS is located “inline” on the firewall.
  - It allows the NIPS to more quickly take action to block an attack.
- Application-aware IPS
  - Know which applications are running as well as the underlying OS.
- Unified Threat Management (UTM): Kaspersky (2019) stated a UTM is an information *security* term that refers to a single *security* solution, and usually a single *security appliance*, that provides multiple *security* functions at a single point on the network.

## Lesson 7.4: How Network Technologies can Enhance Security (04:34)

### *Skills Learned From This Lesson: NAT, PAT, Subnetting IP Addresses*

- Network address translation (NAT) translates the private *IP addresses* of the network in a single public *IP address*. Replaces the private addresses with the public address.
- Port address translation (PAT) which is a variation of NAT. The outgoing packets are given the same IP address but different TCP port numbers.
- Advantage of NAT
  - Masks IP addresses of internal devices
  - An attacker who captures the packet on the internet cannot determine the actual IP address sender.

---

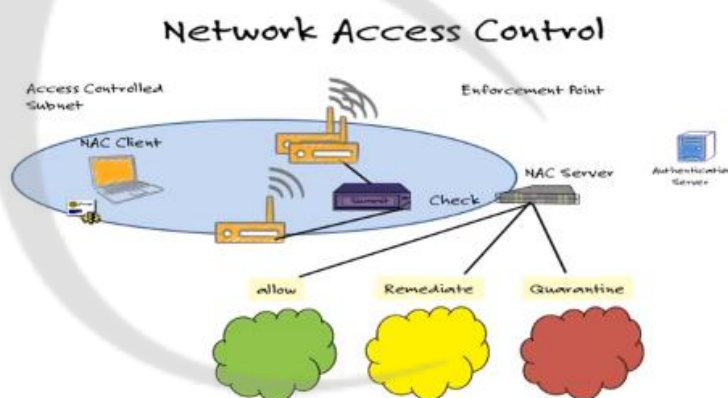
Brought to you by:

**CYBRARY** | FOR BUSINESS

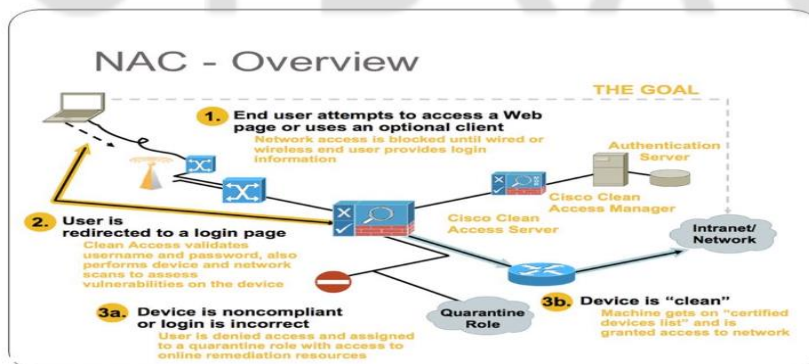
Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Security Through Network Technologies

Class	Beginning address	Ending address
Class A	10.0.0.0	10.255.255.255
Class B	172.16.0.0	172.31.255.255
Class C	192.168.0.0	192.168.255.255



- Network Access Control (NAC) examines the current state or network connection before allowing the network connection. The device must set criteria. If not, NAC allows connections to a “quarantine” network until the deficiencies corrected.



Brought to you by:

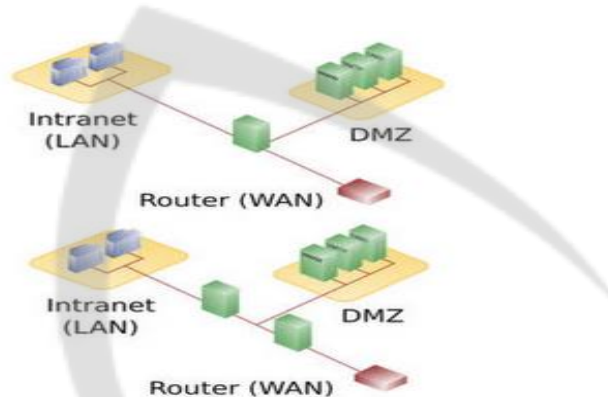
**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Lesson 7.5: Security through Network Design Elements (04:17)

*Skills Learned From This Lesson: DMZ, Subnetting, Remote Access, and Virtual LANs*

- Demilitarized Zone (DMZ) also known as a perimeter network or a screened subnetwork is a physical or logical subnet that separates an internal local area network (LAN) from other untrusted networks.



- Subnetting is used to identify a network and a host on that network. One part is a network address and one part is a host address. It allows a large network to be divided into smaller subnets. Each network can contain several subnets. Each subnet can be connected through different routers. Each subnet contains multiple hosts.
- Virtual LANs (VLAN) - It allows users to be logically grouped together but not physically together on the same network or subnet or switch. Sensitive data can be managed and isolate VLAN members for security. Communication on a VLAN uses a special “tagging” protocol is used for communicating between switches but, if on the same switch. The switch handles the packet transfer.
- Remote Access secured using SSL/TLS not encrypted like a VPN. It can be any combination of hardware and software that enables remote users to access a local internal network.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Module 8: Secure Network Configuration

### Lesson 8.2: Securing Network Infrastructure Devices (15:19)

*Skills Learned From This Lesson: Network Infrastructure Devices, Defining Security Areas, and Recommendations*

- Network Infrastructure Devices are the hardware and software resources of an entire *network* that enable *network* connectivity, communication, operations and management of an enterprise *network*.
- Improving Security Network Infrastructure Devices:
  - Segment and segregate network and functions.
  - Limit unnecessary lateral communications.
  - Harden network devices.
  - Secure access to infrastructure devices.
  - Perform Out-of-Band network management.
  - Validate the integrity of hardware and software.
- Proper network segmentation is an effective security mechanism to prevent an intruder from propagating exploits or laterally moving around an internal network. A poorly segmented network can extend its impact to control critical devices or gain access to sensitive data or intellectual property. Segregation is based on role and functionality.
- Recommendations:
  - Traditional network devices can separate local area network (LAN) segments.
  - Routers can be placed between networks to create boundaries, increase the number of broadcasts, and effectively filter users' broadcast traffic.
  - Implement principles at least privilege and need-to-know when designing network segments.
  - Apply security recommendations and secure configurations to all network segments and network layers.

---

*Brought to you by:*

**CYBRARY** | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

---

# CYBRARY

---

- Virtual Separation of Sensitive Information- It is logical isolation of networks on the same physical network. Virtual segmentation uses the same design principles as physical segmentation but requires no additional hardware.
- Recommendations:
  - Use private virtual LANs to isolate a user from the rest of the broadcast domains.
  - Use virtual routing and forwarding (VRF) technology to segment network traffic over multiple routing tables simultaneously on a single router.
  - Use virtual private networks (VPNs) to securely extend a host/network by tunneling through public or private networks.
- Limit Unnecessary Lateral Communications: Allowing unfiltered peer-to-peer communications, including workstation-to-workstation, creates serious vulnerabilities and can allow a network intruder's access to spread easily to multiple systems. Once an intruder establishes an effective beachhead with the network, unfiltered lateral communications allow the intruder to create backdoors throughout the network.
- Recommendations:
  - Restrict communications using host-based firewall rules to deny the flow of packets from other hosts in the network. The firewall rules can be created to filter on a host device, user, program, or internet protocol (IP) address to limit access from services and systems.
  - Implement a VLAN Access Control List (VACL), a filter that controls access to and from VLANs. VACL filters should be created to deny packets the ability to flow to other VLANs.
  - Logically segregate the network using physical or virtual separation, allowing network administrators to isolate critical devices onto network segments.
- Harden Network Devices: It is a fundamental way to enhance network infrastructure security is to safeguard networking devices with secure configurations. Administrators should implement the following recommendation in conjunction with laws, regulations, site security policies, standards, and industry best practices.
- Recommendations:
  - Disable unencrypted remote admin protocols used to manage network infrastructure.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- Disable unnecessary services.
  - Use SNMPv3 (or subsequent version), but do not use SNMP community strings.
  - Secure access to the console, auxiliary, and virtual terminal lines.
  - Implement robust password policies, and use the strongest password encryption available.
  - Protect routers and switches by controlling access lists for remote administration.
  - Back up configurations and store them offline. Use the latest version of the network device operating system and keep it updated with all patches.
  - Periodically test security configurations against security requirements.
  - Protect configuration files with encryption or access controls when sending, storing, and backing up files.
  - Limiting administrative privileges for infrastructure devices is crucial to security because intruders can exploit administrative privileges that are improperly authorized, granted widely, or not closely audited.
  - Adversaries can use these compromised privileges to traverse a network, expand access, and take full control of the infrastructure backbone.
  - Organizations can mitigate unauthorized infrastructure access by implementing secure access policies and procedures.
  - Implement multi-factor authentication (MFA).
  - Managed privileged access.
  - Manage administrative credentials.
  - Implement current best practices for your network. Practices can change from time to time or possible practices not implemented yet.
- Out-of-Band (OoB) management uses alternate communications paths to remotely manage network infrastructure devices. It provides security monitoring and can perform corrective actions without allowing the adversary (even one who has already compromised a portion of the network) to observe these changes. It can be implemented physically, virtually, or through a hybrid of the two. Using access to manage the network infrastructure will strengthen security by limiting access and separating user traffic from network management traffic.
- Recommendations:
    - Segregate standard network traffic from management traffic.
    - Ensure that management traffic on devices comes only from OoB.
    - Apply encryption to all management channels.

---

# CYBRARY

---

- Encrypt all remote access to infrastructure devices such as a terminal or dial-in servers.
  - Manage all administrative functions from a dedicated, fully patched host over a secure channel, preferably on OoB.
  - Harden network management devices by testing patches, turning off unnecessary services, etc.
  - Monitor the network and review logs.
  - Implement access controls that only permit required administrative or management services.
- Validate Integrity of Hardware and Software:
  - Illegitimate hardware or software presents a serious risk to users' information and the overall integrity of the network. Compromised hardware and software can affect network performance and compromise the confidentiality, integrity, or availability of network assets.
- Recommendations:
  - Maintain strict control of the supply chain and purchase only from authorized resellers.
  - Requires resellers to enforce integrity checks of the supply chain to validate hardware and software authenticity.
  - Upon installation, inspect all devices for a sign of tampering.
  - Validate serial numbers from multiple sources.
  - Download software, updates, patches, and upgrades from validated sources.
  - Perform hash verification, and compare values against the vendor's database to detect unauthorized modification to the firmware.
  - Monitor and log devices- verifying network configurations of devices- on a regular schedule.
  - Train network owners, administrators, and procurement personnel to increase awareness of grey market devices.
- Hardening Network Infrastructure
  - Create a security baseline
  - Harden network devices
  - Ensure firmware is up to date and securely configured
  - Allocate network addresses carefully

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.



- Use security features on routers and switches
  - Enable port security on Ethernet switches and MAC address filtering on WAPs.
  - Enable ARP inspection to protect against ARP spoofing or poisoning attacks.
  - Enable ARP inspection to protect against ARP spoofing or poisoning attacks.
  - On switches, enable DHCP snooping
  - On routers, configure ACLs.
  - Enable loop protection and flood guard features.

## Lesson 8.3: Securing Communications (07:09)

### *Skills Learned From This Lesson: Media Conferencing, Remote Access, and VOIP Security*

- Unified communication systems- “an industry term that describes all forms of business communication, audio, video, multimedia data, text, and messaging.
- Web Conferencing:
  - Use a reputable vendor.
  - Apply sufficient security controls for file sharing.
  - Utilize invite passwords.
  - Keep communication inside the corporate network and use https when possible.
  - Ensure an accurate roll-call.
- Video Conferencing:
  - Disable or cover PC and laptop webcams and microphones when not in use.
- Instant Messaging:
  - Detect unauthorized instant messaging using network devices.
  - Train users to deal with file transfers appropriately.
  - Use a secure channel for authorized IM.
  - SPIM-SPAM over IM.
- Desktop Sharing:
  - Determine authorized access beforehand and block unauthorized.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- Audit for unauthorized access attempts.
- Train users to prepare for sharing by removing sensitive data.
- Remote Assistance:
  - Audit and monitor those that have access.
- Presence
  - It allows others to see a person's availability only on a need to know.
  - Determine the cost versus the benefit of ensuring.
- Email
  - Train users to be prepared for spear phishing, links, and attachments.
  - Implement secured and encrypted transfers when feasible.
- Telephony
  - Change default PBX passwords.
  - Audit access attempts.
- VOIP Security
  - Voice transmitted using Internet Protocol.
  - Employ encryption when the overhead does not lead to quality loss.
  - Ensure physical protection on network ports to reduce the risk of replicating ports and copy unencrypted traffic.
  - Segment VoIP traffic using VLANS to increase the quality of the signal and security.
  - Consider the security of the physical device being used for VoIP.
- Remote Access
  - Ensure that authentication credentials are not intercepted.
  - Implement proper access controls.
    - Radius
    - Diameter
  - Consider network-aware products that enable a different set of firewall rules outside of the corporate network.
  - Monitor remote access attempts and data transactions.

- Enterprise Configuration Management of Mobile Devices
  - Determine the risk versus the benefit and how much access is necessary.
  - Consider implementing the following:
    - The ability to remotely wipe the device.
    - Personal and corporate data separation.
    - Application whitelisting/blacklisting.
    - Mandatory user training.
    - The ability to disable unnecessary services.
    - Configuration management.
- Secure External Communications
  - VPN (Virtual Private Networks) can secure otherwise non-secure protocols such as HTTP, SMTP, and FTP.
  - Avoid treating VPN clients in the same manner as typical PCs as they may be compromised with malware.
  - VPN types:
    - Layer 2 Forwarding
    - L2TP (Layer 2 Tunneling Protocol)
    - PPTP (Point-to-Point Tunneling Protocol)
    - IPSec (Internet Protocol Security)
- Secure Implementation of Collaboration Platforms
  - Collaboration tools historically implement limited security
  - Authenticate all users prior to use
  - Implement role-based access control to ensure need to know
  - Log the overall system and individual content access attempts
  - Apply data loss procedures and tools.
- Prioritizing Traffic (QoS)
  - QoS (Quality of Service) prioritizes network traffic based on business needs.
  - UDP services such as Voice and video can handle packet loss while TCP services such as HTTP and SMTP cannot.
  - QoS architectures
    - Integrated Service- Uses RSVP (Resource Reservation Protocol) to tell other network devices to set some traffic as “guaranteed” or high priority beforehand.

- Differentiated Services- Service prioritization information is sent with the actual traffic packets.

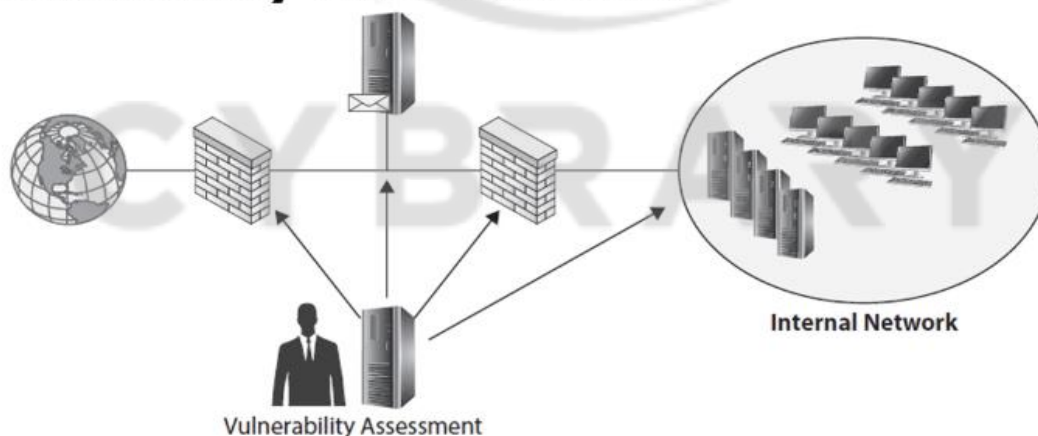
## Module 9: Scanning and Monitoring

### Lesson 9.2: Perform Security Assessment Activities (06:40)

*Skills Learned From This Lesson: Security Audit, Vulnerability Assessments, and Penetration Testing*

- An information security audit is a systematic, measurable security audit of how the organization's security policy is employed. Testing is the process of exercising specific security objectives under specified conditions to compare actual and expected behaviors.
- Information security audits can be internal or external and consist of
  - Preparation
  - Scheduling
  - Evaluation-performing audit
  - Formal response- reporting

## Vulnerability assessments



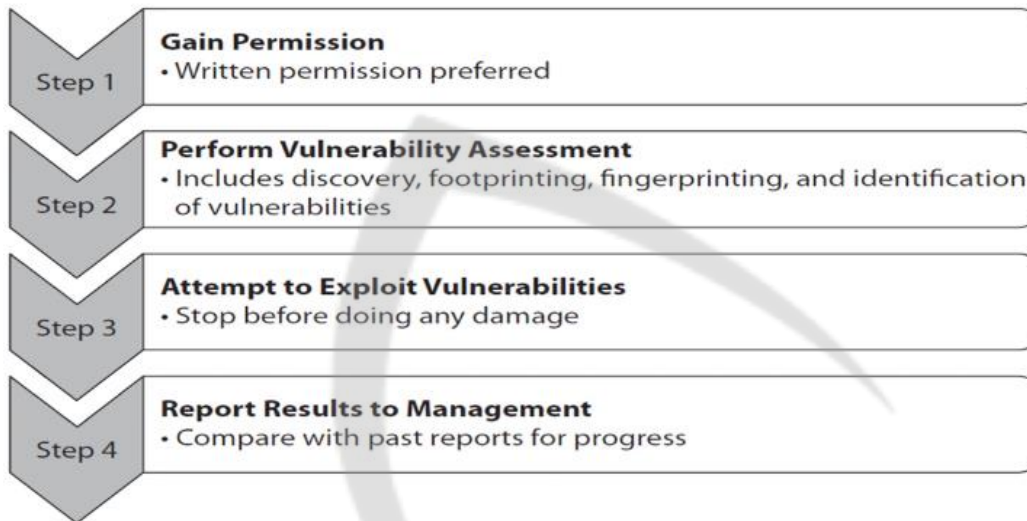
---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Penetration tests



Lesson 9.3: Operate and Maintain Monitoring Systems (09:49)

*Skills Learned From This Lesson: Log Management, Log Analysis, and SEIM*

- Events of Interest:
  - 1. Authentication and Authorization Reports
  - 2. System and Data Change Reports
  - 3. Network Activity Reports
  - 4. Resource Access Reports
  - 5. Malware Activity Reports
  - 6. Failure and Critical Error Reports

---

Brought to you by:

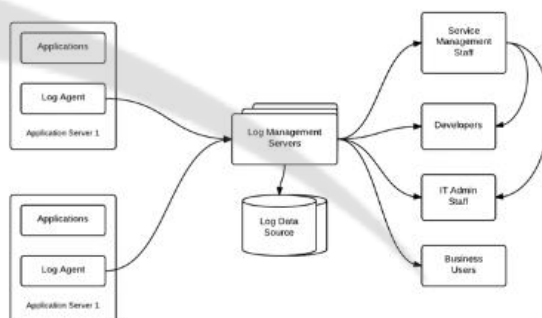
**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Log Management

- Managing the record of events occurring within an organization's systems and networks

- Log Generation and Storage
- Log Protection
- Log Analysis



- Log Generation
  - Log Configuration- Determines what to log:
    - Host-based activity
    - Network activity
  - Clipping Levels- A disk's ability to maintain all of the magnetic properties and retain data.
    - False Positives
    - False Negatives
  - Time Synchronization
    - Network Time Protocol (NTP) - It is clock synchronization between computer systems over the packet and variable-latency data networks.

### Log Generation

- Log Storage
  - Centralized storage
  - Excessive logging
    - Stop logging
    - Overwrite oldest log entries
    - Stop log generator
  - Retention



Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- Log Protection
  - Limit access to a log file.
  - Avoid recording unneeded sensitive data.
  - Protect archived log files.
  - Secure the process that generates the log entries
  - Critical systems should log to another system.
  - Configure each log source to behave appropriately when logging errors occur.
- Log Analysis
  - Event Correlation
    - Automation
    - Context
    - Prioritization
      - Entry type
      - The newness of the entry type
      - Log source
      - Source or destination IP address
      - Time of day or day of the week
      - Frequency of the entry
- Security Information and Event Management (SEIM) is defined as a complex set of technologies brought together to provide a holistic view into a technical infrastructure:
  - Event and log collection
  - Layered centric views or heterogeneous
  - Normalization
  - Correlation
  - Adaptability (Scalable)
  - Reporting and alerting
  - Log management

## Lesson 9.4: Analyze Monitoring Results (08:02)

*Skills Learned From This Lesson: Security Analytics, Data Visualization, and Event Data Analysis*

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Security Analytics, Metrics, and Trends

- Security is first layer of a defense-in-depth approach is the enforcement of the fundamental elements of network security.
- Analytics is the discovery and communication of meaningful patterns in data. Especially valuable in areas rich with recorded information, analytics relies on the simultaneous application of statistics, computer programming, and operations research to quantify performance.
- Metrics and analysis (MA) is a sophisticated practice in security management that takes advantage of data to produce usable, objective information and insights that guide decisions.
- Trends is a pattern of gradual change in a condition, output, or process, or an average or general tendency of a series of data points to move in a certain direction over time, represented by a line or curve on a graph

## Visualization

- Data visualization is a general term that describes any effort to help people understand the significance of data by placing it in a visual context. Patterns, trends and correlations that might go undetected in text-based data can be exposed and recognized easier with data visualization software.
  - "...to convey information through visual representations."
  - "...produces (interactive) visual representations of abstract data to reinforce human cognition; thus enabling the viewer to gain knowledge about the internal structure of the data and causal relationships in it."
- Visualization Goals:
  - Answer questions (or discover them).
  - Make decisions.
  - See data in context.
  - Support graphical calculation.
  - Find patterns.
  - Present arguments or tell a story.
  - Inspire.
- Three Functions of Visualization
  - Record: Store information.
  - Analyze: Supporting reasoning about information.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.



- Communicate: Convey

## Data visualization tools

- **Dygraphs**-A fast, flexible open source JavaScript charting library that allows users to explore and interpret dense data sets. It's highly customizable, it works in all major browsers, and you can even pinch to zoom on mobile and tablet devices.
- **ZingChart**-is a JavaScript charting library and feature-rich API set that lets you build interactive Flash or HTML5 charts. It offers over 100 chart types to fit your data.
- **InstantAtlas**-Enables you to create highly interactive dynamic and profile reports that combine statistics and map data to create engaging data visualizations
- **Visual.ly** -Visual.ly is a combined gallery and infographic generation tool. It offers a simple toolset for building stunning data representations, as well as a platform to share your creations.

## Event data analysis

- The National Institute of Standards and Technology (NIST) states:
  - A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network.
    - Organizations should establish policies and procedures for log management.
    - Organizations should prioritize log management appropriately throughout the organization.
    - Organizations should create and maintain a log management infrastructure
    - Organizations should provide proper support for all staff with log management responsibilities.
    - Organizations should establish standard log management operational processes
- Packet Dump is a computer networking term for intercepting a data packet that is crossing or moving over a specific network.
- Machine Data- is digital information created by the activity of computers, mobile phones, embedded systems, and other network services.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the *fastest growing catalog* in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

---

- Communication Findings- Are a result of data analysis can be communicated using a number of methods. The decision as to the medium or media to be used to convey the information is directly related to the speed of the communication.
  - Solid substance
  - Sound logic
  - Balance tone
  - Visual clarity
  - Good mechanics

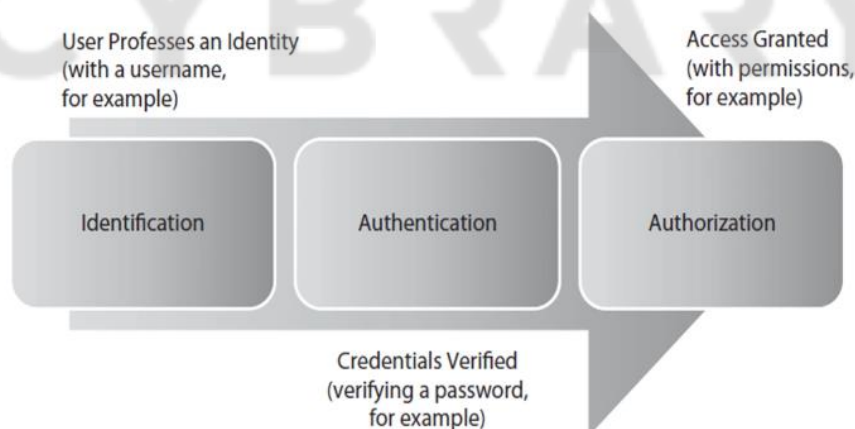
## Module 10: Scanning and Monitoring

### Lesson 10.2: Implement Authentication Mechanisms (21:05)

*Skills Learned From This Lesson: Different Access Controls, Access Control Terminology, and Access Control Process*

- Different Access Control
  - Access Control- Granting or denying approval to use specific resources.
  - Physical Access Control- Consists of fencing, hardware doors locks, and mantraps to limit contact with devices.
  - Technical Access Control- Consists of technology restrictions that limit users on computers from accessing data.

### Identification, Authentication, and Authorization



---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Access Control Terminology

Action	Description	Scenario example	Computer process
Identification	Review of credentials	Delivery person shows employee badge	User enters user name
Authentication	Validate credentials as genuine	Gabe reads badge to determine it is real	User provides password
Authorization	Permission granted for admittance	Gabe opens door to allow delivery person in	User authorized to log in
Access	Right given to access specific resources	Delivery person can only retrieve box by door	User allowed to access only specific data

## Steps of Access Control Process

Access control requires:

- Identification
- Authentication
- Authorization



Access control process:

- ▷ **Subject:** presents credentials to the system
- ▷ **Authentication:** system verifies and validates that the credentials are authentic
- ▷ **Authorization:** grants permission to allowed resources

Brought to you by:

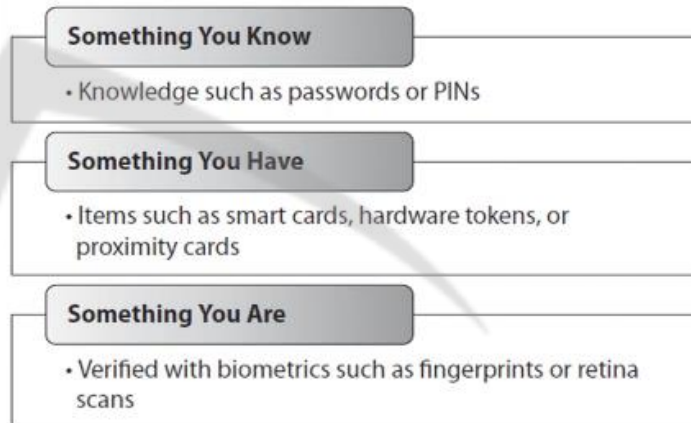
**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Exploring Authentication

- Three Factors of Authentication

- Something you know
- Something you have
- Something you are



## Exploring Authentication

- Something you know

- Static password
- One-time or dynamic password
- Cognitive password

Password Type	Definition
Cognitive	Cognitive data that the user knows such as mother's maiden name or favorite color
Dynamic	Passwords that change upon each consecutive login
One Time	Passwords that are only valid for a single use and are thereafter useless
Passphrase	A password based on a group of words or phrase
Static	A normal password which is only changed on request

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- Software tokens and one-time passwords
  - HOTP
  - TOTP
  - OPIE
  - S/Key
- Something you are (biometrics)
  - Fingerprint and thumbprint
  - Palm
  - Retina
  - Iris
- Multifactor Authentication refers to using at least two different types of factors for authentication purposes. The two types of authentication factors might be a typed-in password and a thumbprint.
- Multifactor Authentication
  - A smart card ( something you have) and a PIN (something you know)
  - A fingerprint (something you are) and a password (something you know)
  - A hardware token (something you have) with a username and password (something you know)
- Single Factor authentication is only one factor is used. Requiring the entry of two or more of the same type of factor is also regarded as single-factor authentication.
- Kerberos- It is a network protocol that uses secret-key cryptography to authenticate client-server applications.
  - An attacker would attempt to compromise the Kerberos servers.
  - Exploit outdated software in the infrastructure.
  - Alternative attack methods could include replay attacks and password-guessing.
- Single Sign-on Authentication
  - Federated access
  - SAML
    - Principal

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

# CYBRARY

- Identity provider
- Service provider
- SESAME
- KryptoKnight

## Exploring Authentication

- Centralized vs. decentralized authentication



- Offline authentication

Decentralized Authentication  
Four Passwords Needed for Four Systems

Centralized Authentication  
One Password Needed

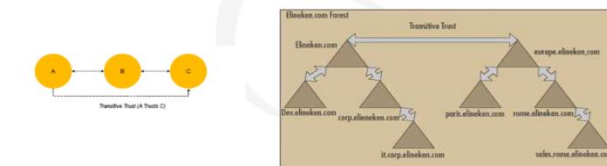
- Token-Based Access Controls Are usually a small hardware device that displays a number. It checks against a database for changes. When a user wants to log in or access any application they enter the number that is visible at the moment. It is authenticated against the authentication server of the number displayed on the token.

### Lesson 10.3: Operate Internetwork Trust Architectures (08:11)

*Skills Learned From This Lesson: Trust Transitivity, One-Way Trust, Two-Way Trust, and Transitive Trust*

#### Trust Transitivity

- Transitivity determines whether a trust can be extended outside the two domains between which the trust was formed.



Brought to you by:

**CYBRARY** | FOR BUSINESS

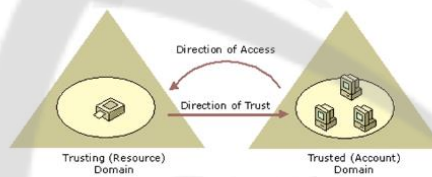
Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.



- Trusted Systems: Mandatory access control (MAC) is traditionally enforced by the system through the use of a trusted computer base (TCB). This is a protected computing system that includes a security kernel and a reference monitor.

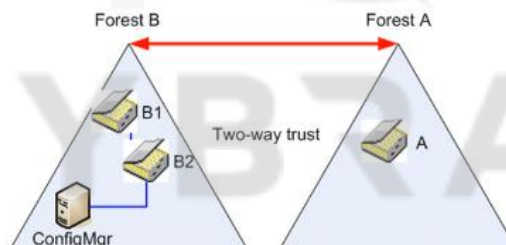
## One-Way Trust

- A **one-way trust** is a unidirectional authentication path created between two domains (**trust** flows in **one** direction, and access flows in the other).



## Two-Way Trust

- A two-way trust can be thought of as a combination of two, opposite-facing one-way trusts, so that, the trusting and trusted domains both trust each other (trust and access flow in both directions).



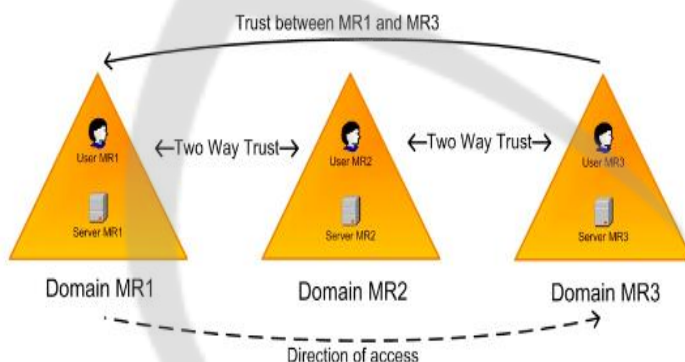
Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Transitive trust

- **Transitive trust** is a two-way relationship automatically created between parent and child domains in a Microsoft Active Directory forest.



### Lesson 10.4: Participate in the Identity Management Lifecycle (06:56)

*Skills Learned From This Lesson: Authorization, Proofing, and Provisioning*

- Authorization is a security mechanism to determine access levels or user/client privileges related to system resources including files, service, computer programs, data and application features.
- Proofing is the identity of a subject system, usually in the form of a user ID.
  - Distinguishes between different subjects and objects
  - Allows for accountability
  - Allows for the assignment of rights
  - May be used in conjunction with authentication to prove the identity provided is valid.
- Provisioning is a process to create, modify, disable and delete users or accounts to include profiles within an information technology infrastructure and associated

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.



applications.

- Maintenance like account lockout policies, thresholds, and duration on accounts. Entitlement is the principle of least privileges.
- De-provisioning is the act of removing access from and freeing up resources reserved by end-users and their file transfer workflows. Disable or delete.

## Lesson 10.5: Implement Access Controls (08:26)

*Skills Learned From This Lesson: Access Control Model, Comparing Access Control Model and, Access Control Permissions*

- Subjects and Objects:
  - A subject is a user or entity taking the action or accessing a resource such as a database.
  - An object
- Access Control Model- Standards that provide a predefined framework for hardware or software developers. Use the appropriate model to configure the necessary level of control. There are four major control models:
  - Mandatory Access Control (MAC)
  - Discretionary Access Control (DAC)
  - Role-Based Access Control (RBAC)
  - Rule-Based Access Control (RBAC)
- Mandatory Access Control (MAC)
  - Restriction based on the information's sensitivity.
  - Makes use of classifications and security labels.
  - The system enforces classification labels and need-to-know
  - This model lacks the flexibility to change/ adapt over time, but provides for a more secure environment, enforced by the system, not people.
  - Requires data classification.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Comparing Access Control Models

- Mandatory Access Control models
  - Bell-LaPadula-This model enforces information confidentiality
  - Biba-This information model is an information integrity model.
  - Clark-Wilson-This model enforces separation of duties through integrity rules.
  - Chinese Wall-The basic **model** used to provide both privacy and integrity for data is the "**Chinese Wall Model**" or the "Brewer and Nash **Model**". It is a **security model** where read/write access to files is governed by membership of data in conflict-of-interest classes and datasets.

Model	Goal	Rules
Bell-LaPadula	Confidentiality	No read up, no write down
Biba	Integrity	No read down, no write up
Clark-Wilson	Integrity	Certification (C) rules and enforcement (E) rules
Chinese Wall	Prevent conflict of interest	Access governed by membership in groups to prevent conflicts of interest

- Discretionary Access Control (DAC)
  - The most common access control method
  - Permissions set by the data owner
  - Supports the concept of need-to-know
  - More flexible than Mandatory Access Control (MAC), but with an increased risk of unauthorized disclosure of information.
- A most common implementation of DAC is the use of objects, subjects, and permissions.
  - Subjects: can be individuals, groups or processes.
  - Permissions: such as read, write, append, delete, and execute.
- Some operating systems allow for more "granularity"- more options for permissions.
- Access Control Groups:
  - ACL permissions should be based on groups when possible. Sequence number.

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

---

- Management of ACL's is much easier when in groups.
- People working in a similar area will require similar access.
- Access Control Permissions: Permissions can be inherent, granted, or inherited.
  - Inherent rights like system and admin rights can bypass security policies.
  - Users can be granted admin and system privileges
  - Inherited permissions are those that are propagated to an object from a parent object.
- Permissions should be based on organizational policy and the sensitivity of the information.
- Non-Discretionary Access Control:
  - Technically not MAC or DAC, but may have attributes of both.
  - Often supplementary when data owner not defined.
  - Managed by a System Administrator versus a Data Owner.
  - Enforced by the Operating System.
- Role-Based Access Control (RBAC)
  - Permissions are assigned to roles rather than to individual users.
  - Users are assigned to roles rather than directly to permissions.
  - RBAC is good for a company that has high employee turnover.
- Permissions are assigned to roles rather than to individual users.
  - Neither DAC nor MAC.
  - Examples:
    - Routers and firewalls.
    - Time-Based- access based on a specified period of time a subject can access an object.
- Attribute-based Access Control (ABAC) can control access based on three different attribute types: user attributes, attributes associated with application or system to be accessed, and current environmental conditions.
  - An example of ABAC would be allowing users who are type= employees and have department= HR to access the HR/Payroll system and only during business

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

hours within the same time zone as the company.

- ABAC enables fine-grained access control, which allows for more input variables into an access control decision. Any available attribute in the directory can be used by itself or in combination with another to define the right filter for controlling access to a resource.

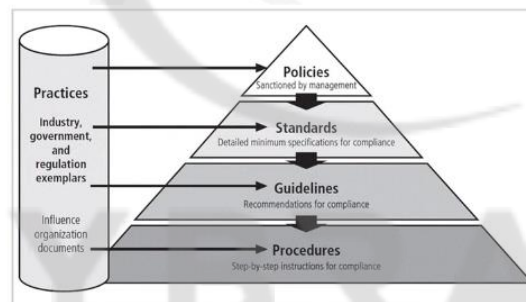
## Module 11: Incident Response

### Lesson 11.2: Participate In Incident Handling (12:31)

*Skills Learned From This Lesson: Incident Response Policy, Implementation of Countermeasures, and Incident Response Planning*

#### Incident response policy

- The incident response policy is part of the overall IT security policy for the organization.



The incident response policy is part of an overall IT security policy for the organization.

- Incident Response Policy
  - Preparation- Planning in advance on how to handle and prevent security incidents.
  - Detection & Analysis- Encompasses everything from monitoring potential attack vectors to looking for signs of an incident, to prioritization.
  - Containment Eradication & Recovery- Developing a containment strategy, identifying and mitigating the hosts and systems under attack, and having a plan for recovery.

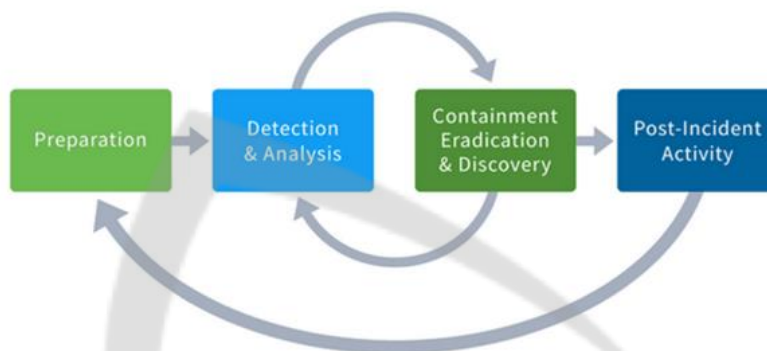
---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- Post- Incident Activity- Reviewing lessons learned and having a plan for evidence retention.



*Figure 1 – The NIST recommended phases for responding to a cybersecurity incident*

- Incident Response planning includes identification of, classification of, and response to an incident.
- Attacks classified as incidents if they:
  - Are directed against information assets
  - Have a realistic chance of success
  - Could threaten confidentiality, integrity, or availability of information
- Incident response (IR) is more reactive than proactive, with the exception of planning that must occur to prepare IR teams to be ready to react to an incident.
- Incident response policy identifies the following key components:
  - Statement of management commitment
  - Purpose/ objectives of the policy
  - Scope of policy
  - Definition of InfoSec incidents and related terms
  - Organizational structure
  - Prioritization or severity rating of incidents
  - Performance measures
  - Reporting and contact forms

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- Incident Planning
  - Predefined responses enable the organization to react quickly and effectively to the detected incident if:
    - The organization has an IR team
    - The organization can detect the incident
  - IR team consists of individuals needed to handle systems as an incident takes place.
- Incident response plan
  - Format and content
  - Storage
  - Testing
- Incident detection/discovery
  - A most common occurrence is compliant about technical support, often delivered to help desk.
  - Careful training is needed to quickly identify and classify an incident.
  - Once an incident is properly, the organization can respond.
  - Incident indicators vary.
- Incident reaction:
  - Consists of actions that guide the organization to stop the incident, mitigate its impact, and provide information for recovery
  - Actions that must occur quickly:
    - Notification of key personnel
    - Documentation of the incident
- Incident containment strategies:
  - Containment of incident's scope or impact as the first priority; must then determine which information systems are affected.
  - An organization can stop incidents and attempt to recover control through a number of strategies.
- Incident recovery
  - One incident has been contained and control of systems regained, the next stage is recovery.

- The full extent of the damage must be assessed.
- The first task is to identify the human resources needed and launch them into action.
- Organization repairs vulnerabilities address any shortcomings in safeguards and restore data and services of the systems.
- Escalation management involves transferring issues to a higher level of management. A common example amongst organizations might exist as follows:
  - Internal
    - Senior Management
  - External Agencies
    - Homeland Security
    - Regulatory Agencies
    - Law Enforcement
    - Customers

## Implementation of Countermeasures

- A countermeasure is an action or method that is applied to prevent, avert or reduce potential threats to computers, servers, networks, operating systems (OS) or information systems (IS). Countermeasure tools include anti-virus software and firewalls.
- Countermeasures are usually put in place as a response to a risk analysis. Example include
  - Routers: Mask Internet Protocol (IP) addresses
  - Anti-virus and anti-spyware applications: Protect against malicious software (malware), including viruses, Trojans and adware
  - Behavioral techniques: Applied by users to deter threats, such as suspicious email attachments
  - Firewalls: Facilitate authorized network access
  - Intrusion detection systems (IDS): Prevent and/or block unauthorized system access
  - Physical security (especially in enterprises): Prevents hacking and network subterfuge

### Lesson 11.3: Understand and Support Forensic Investigations (08:21)

*Skills Learned From This Lesson: Digital Forensics, Forensic Investigation, and Forensic Guidelines*

- Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- Forensic investigation is the gathering and analysis of all crime- related physical evidence in order to come to a conclusion about a suspect. Investigators will look at blood, fluid, or fingerprints, residue, hard drives, computers, or other technology to establish how a crime took place.
- Locard's exchange principle holds that any perpetrator of an intrusion leaves behind trace evidence within the system. This trace evidence may be used to identify the attacker.
- Computer Forensic Guidelines for Investigations:
  - Identifying Evidence
  - Collecting or Acquiring Evidence
  - Examining or Analyzing Evidence
  - Presentation of Evidence and Findings
- Evidence Collection- To identify, label, record, and acquire data from, the possible sources of relevant data, while following guidelines and procedures that preserve the integrity of the data.
- Preservation- Prevent spoliation, which is the destruction or alteration of evidence when an investigation or litigation is either in process or might come to pass in the future.
- Digital Forensic Techniques:
  - BitStream Image
  - Log Monitoring
  - Data Recovery
  - File Header Investigation



## Evidence Life Cycle



## Digital Forensic Tools

Name	Platform	License	Description
Autopsy	Windows, macOS, Linux	GPL	A digital forensics platform and GUI to The Sleuth Kit
COFEE	Windows	proprietary	A suite of tools for Windows developed by Microsoft
Digital Forensics Framework	Unix-like/Windows	GPL	Framework and user interfaces dedicated to Digital Forensics
EPRB	Windows	proprietary	Set of tools for encrypted systems & data decryption and password recovery
EnCase	Windows	proprietary	Digital forensics suite created by Guidance Software
FTK	Windows	proprietary	Multi-purpose tool, FTK is a court-cited digital investigations platform built for speed, stability and ease of use.
ISEEK[2]	Windows	proprietary	Hybrid-forensics tool running only in memory - designed for large networked environments
IsoBuster	Windows	proprietary	Essential light weight tool to inspect any type data carrier, supporting a wide range of file systems, with advanced export functionality
Netherlands Forensic Institute / Xiraf[3]	n/a	proprietary	Computer-forensic online service.
Open Computer Forensics Architecture	Linux	LGPL/GPL	Computer forensics framework for CF-Lab environment
OSForensics	Windows	proprietary	Multi-purpose forensic tool
PTK Forensics	LAMP	proprietary	GUI for The Sleuth Kit
SafeBack[6]	N/a	proprietary	Digital media (evidence) acquisition and backup

- Chain of custody refers to a forensic principle whereby each movement or transfer of data must be recorded and logged appropriately.
- At no time must the chain be disrupted; if it is, the evidence is of no use.

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

---

- Evidence should be appropriately identified, including the circumstances under which it was collected, who collected it, a detailed description, and other important information.
- In most cases, the evidence is packed in poly bags for transport to a forensic laboratory or storage location.
- While the forensic examiner is performing the examination of the evidence, they will allow the character of the evidence to lead to various suppositions and potential conclusion possibilities.
- This is the interpretation process that forensic experts will use to determine the importance or significance of various pieces of evidence information.

CYBRARY

---

*Brought to you by:*

**CYBRARY** | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*