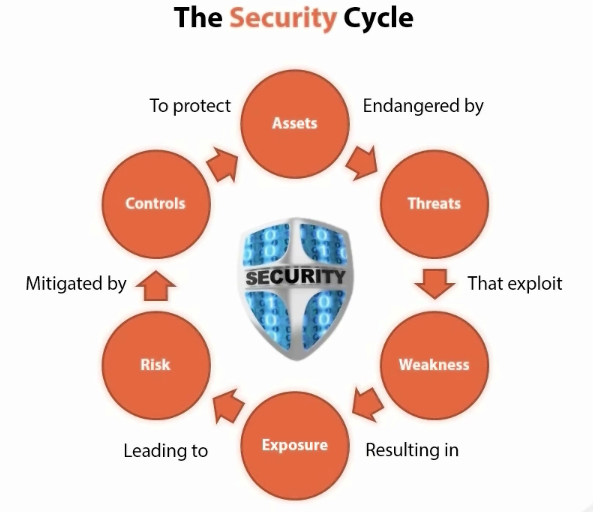
# CompTia Notes: Compliance and Operational Security

* Module Overview
  + Importance of Risk, risk calculation, loss, etc.
  + Managing risk, annual loss, single event loss
  + NIST Special Publication 800-53:
    - National Institute of Standards has recommended security controls for federal information systems
    - Protects “CIA triad”:
      * Confidentiality
      * Integrity
      * Availability
  + The Security Cycle 
  + Control Types
    - Important that organizations have a written security policy
    - Important to have contingency planning and incident response
    - Physical and personnel security
    - Awareness and training
    - Change/configuration management in place to make sure changes don’t create any problems where a change in one area affects another
  + Creating Incident Response plan
    - Preparation, detection and analysis, Containment Eradication and Recovery, Post-Incident activity
    - Average time to contain a cyber-attack is 31 days
    - Average cost of cyber-crimes is 7.6 million per year
  + Important policies to have
    - Privacy policy
    - Acceptable use policy
    - Security policy
    - Mandatory vacations
    - Job rotation(make sure people that get rotated don’t retain their previous privlidges
    - Separation of duties (separation of powers-> checks and balances)
    - Least privilege
  + Why mandatory vacations
    - Keeps personnel away from company assets for a period of time (allows companies to see anomalies) doesn’t allow people who are doing fraud, theft, etc to cover their tracks
    - Allows another person to step in to do things the right way and see if the other person was really doing their job correctly
  + Risk Calculation
    - How often will the issue occur?
    - How much will it cost?
    - What is the likelihood that it will happen?
    - Quantitative analysis assigns an exact monetary value to assets, attempts to give expected yearly loss in dollars for any given risk, enables prioritization based on cost
    - ALE: Annual Loss Expectancy
    - SLE: Single Loss Expectancy = asset value x Exposure factor
    - Annualized rate of Occurrence
  + Other terms
    - MTTF: Mean time between failures, statistical average a device lasts between failures
    - MTTR: Mean time to failure, statistical average of how long a component lasts, referring to things that will be replaced rather than repaired
    - MTBF: Mean time to repair
* Risk Management/Mitigation Concepts
  + - Risk Transference by using a hosted provider or insurance company
    - Risk Acceptance: what is the cost of removing the risk vs. dealing with the issue if/when it occurs “juice isn’t worth the squeeze”
    - Risk Mitigation/deterrence
    - Risk Avoidance: Opting not to do something because the risk is too high
  + Disable (don’t delete) accounts that aren’t in use so you can go back and access their files if necessary
  + Perform Routine Audits
    - Identify Opportunities to reduce risk
      * Ensure compliance
      * Identify users with too many rights
      * Identify users who can perform more than one job
  + Preventing data loss or theft
    - PII: Personally Identifiable Information
    - Very important to keep safe and make sure it isn’t leaked
    - Encrypt data at rest and in transit
      * VPN
      * TSL
  + Attack Vectors
    - Data can be stolen from a variety of locations
      * Access to a user’s laptop or desktop
      * Sniffing unencrypted communication
      * Stealing removable media, smartphones
  + Data Loss Prevention tools
    - Scan file shares and network traffic of PLL
    - Many NextGen Firewalls have DLP technology built-in
    - Software can also be used to scan traffic (emails) and detect use of flash drives
* Implementing Basic Forensic Procedures
  + What is Computer Forensics?
    - Analysis of digital data
    - Must be done in a predetermined fashion to not tamper with evidence already there accidentally
  + Order of Volatility
    - Computer Evidence is stored in a number of locations
      * RAM has a short lifespan
      * Magnetic hard disks are more long term and the files live on even after being deleted
      * Some are long-term, but are irretrievable once deleted (SSD flash drives)
      * Data should be gathered based on the life expectancy of the data

1.CPU, cache and register content

1. Routing table, ARP cache, process table, kernel statistics
2. Memory

4. Temporary file system/ swap space

5. Data on Hard disk

1. Remotely logged data

7. Data contained on archival media

* + First Responder Best Practices
    - Photograph the computer and scene
    - If the computer is off do not turn it on
    - If it is on, don’t turn it off – photograph the screen
    - Connect via usb and image the computer (order of volatility) to get an exact duplicate
    - Separate person from the device
    - Collect live data -start with RAM image
    - Collect local image of hard drisk using forensic tools: dd.exe, Helix3, EnCase, F-Response
    - Then remove battery or unplug power chord
  + Capture a System Image
    - Live USB can be used to boot and write protect target computer (Kali linux, EnCase, access data)
    - Make multiple copies of the imaged data and only use copies to perform the investigation and analysis
    - Forensic software will log and timestamp every action taken during the investigation, helps to build a case folder
  + Network Traffic and Logs
    - IP addresses can be used to locate the source and destination of an event
    - Logs are generated by a variety of devices
      * Desktops and laptops
      * Shows when files were accessed, who was logged on when, what changes were made
      * Routers, switches, firewalls create log files
      * Smart phones and gaming consoles
  + Capture Video
  + Record Time Offset
    - Must ensure time offset is recorded so event correlation can be properly documented
    - When analyzing data, logs, syslogs, configuration files and other evidence, be sure to record the offset from UTC (coordinated universal time)
  + Take Hashes
    - Hash is taken prior to imaging
    - Hash is taken again on the resultant image file to confirm that they are both identical
  + Screenshots
    - If you can’t do the other back up methods, taking screen shots is a good last ditch effort
    - Snagit
  + Witnesses
    - Witness accounts can be crucial to an investigation
    - When taking statements document date time, what else was going on, who else was there, equipment present, etc.
  + Tracking man hours and Expense
    - Many companies base next year’s budget off of the current year’s budget
    - Why it is important to track man hours accurately
  + Chain of Custody
    - No gaps in the chain of custody (can destroy a case)
    - Must document who interacts with what evidence and when
    - Custody logs should accompany each piece of evidence
      * Date time location
      * Person checking in/ checking out
      * Seals /tags on evidence bags
  + Big Data Analysis
    - Unstructured data can be parsed and find connections and correlations
    - Can also be used to make trends and predictions based on real-time or historical data.
* Incident Response Concepts
  + Incident Preparation
    - Identify issues (to work on most critical issues first)
    - Patch, upgrade, or bring new systems online
    - Document process and steps taken for future use
    - Use NIST Computer Security Incident Handling guide
    - Set up contingency plans for communication (if email goes down, move to text or calling, etc.)
    - Clear definition of roles responsibilities
  + Incident Identification
    - Identify where or who the attack is coming from
    - Figure out true threats vs. anomalies
      * Limiting false positives and focus on true events
    - Implement IPS/IDS and Big Data analysis tools
  + Incident Response
    - Make sure systems are patched and up to date
  + Incident Notification and Escalation
    - Qucikly assess and triage as appropriate
    - Determine who needs to be notified
      * Security teams
      * CIO/CISO
      * Human Resources, Public Information Office or Public Affairs
      * Legal Teams
      * Social Media teams
  + Incident Mitigation and Isolation
  + Lessons Learned
    - Post Incident Review with everyone involved in an incident
    - Document what happened, what steps were taken, and outcome
    - Knowledge sharing between departments
    - Identify areas for improvement
  + Incident Reporting
    - Keep logs of actions taken as they occur
    - Keep documents objective and fact based
  + Recovery and Reconstitution Procedures
    - What needs to be recovered, might not want to back up from infected files
    - Might be best to build from scratch
  + First Responder
    - Evidence handling procedures must be documented beforehand
      * Things like who to notify, what to document, etc.
  + Incident Isolation
    - Mitigate risk as quickly as possible (but not at the risk of destroying evidence)
    - Get business up and running as fast as possible
    - Quarantine
  + Data Breach
    - Data breaches often incur significant financial loss
    - Once data is gone, recovery is unlikely
    - Determining extent is difficult
    - Loss of customer confidence
    - Determine who needs to be notified
  + Damage and Loss Control
    - Systems in place to remotely wipe compromised systems
    - Use encryption on data
* Security Related Awareness and Training
  + Security Polity Training and Procedures
    - Employees understand what is considered personally Identifiable Information
    - Must verify information first before giving away information
    - Tests and assessments can validate that employees understand the training
    - Must be able to apply the knowledge to specific situations
  + Validate Compliance and Security Posture
  + Role Based Training
    - Employees must be trained for a specific role and only the rights associated to the role should be appropriate but not overly broad
    - Make sure rights are removed when an employee changes roles
  + Personably Identifiable Information
    - Sensitive data that uniquely identifies or is associated with a person
    - Data should be encrypted when in transit or at rest
  + Information Classification
    - Not all data is equal in its sensitivity
    - Public, Corporate, Government
  + Data Labeling, Handling, and Disposal
    - Some data may need to be kept for a long period of time
    - Some might need to be deleted multiple times to be irretrievable
    - Some might need to be certified as destroyed
  + Compliance
    - Important to know and follow regulations and compliance
  + User Habits
    - Password behaviors
      * Don’t make them too complicated while staying secure
      * Train them not to write passwords down, reusing old passwords, kids names, pet names
    - Clean Desk policies
      * Keep confidential or sensitive information off of desks and away from public view
    - Prevent tailgating
      * Don’t be fooled by people carrying items or acting like they belong, don’t hold the door for them
    - Personally owned devices
  + New Threats, Security Trends, and Alerts
    - New viruses come up every day, important to stay updated
    - Phishing attacks
    - Zero-day exploits
  + Use of Social Networking and P2P
    - If a social networking account gets hacked, people are more likely to trust people they know
    - Can inadvertently leak massive amounts of sensitive information if system isn’t set up correctly
* Physical and Environmental Controls
  + Environmental Factors
  + HVAC
    - Important to monitor humidity/heat
  + Fire Suppression
    - FM200 is most common clean agent for fire suppression
  + EMI Shielding
    - Electromagnetic interference
    - Cabling is subject to EMI and crosstalk
    - Shielded Twisted pair provides most protection.
    - Copper cable emanates signal that can be picked up at short distances (why we do end to end encryption)
    - Encryption and secure transport are best defense
  + Hot and Cold Aisles
    - Help reduce heating and cooling
    - HVAC runs more effiently when designed properly
    - Best to place front of system facing each other (cool side) and then opposing aisles go back to back to make a hot aisle for HVAC to pull out.
    - Hot air containment aisles – contain the heat in an aisle
    - Cold aid containment – closed off area where fronts face each other
    - Make sure hot areas are where HVAC is
  + Environmental Monitoring
    - Use sensors to monitor temp, humidity, power, flooding, Airflow and Pressure (positive), motion
  + Temperature and Humidity Controls
    - Controls should be operated separate from the rest of the company
    - Closed loop, positive pressurization system (air is filtered and recycled)
  + Physical Security, Locks, Mantraps, surveillance
    - Hardware locks
  + Fencing
  + Proximity Readers and Access Lists
  + Proper Lighting and Signs
  + Barricades
  + Biometrics
  + Protected Distribution Systems
  + Alarms and Motion Detection