CSF 434/534: Advanced Network and System Security

Week 10 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes

Agreement Types

Agreement Types

Standard operating procedure

- ☑ Important processes to maintain data and system security
  - ☑ Detail routine operations
  - ☑ Usually quite extensive
- ☑ Day-to-day processes
- ☑ New user account creation
  - ☑ Backup data storage requirements
  - ☑ Encryption key requests
- ☑ These should be well documented
  - ☑ Some processes require extensive documentation
  - ☑ Comply with industry regulations

Agreement Types

Interoperability agreements

- ☑ Third-parties and outsourced services
  - ☑ The legal side of information technology
- ☑ Web hosting, payroll services, firewall management, etc.
  - ☑ Some of your data is in the hands of others
  - ☑ Who do they hire?
  - ☑ What type of access controls are in place?
- ☑ Include the legal department with these agreements
  - ☑ It can only help you later

Agreement Types

Common agreements

- ☑ Service Level Agreement (SLA)
  - ☑ Minimum terms for services provided
  - ☑ Uptime, response time agreement, etc.
- ☑ Business Partners Agreement (BPA)
  - ☑ Commonly seen between manufacturers and resellers
- ☑ Interconnection Security Agreement (ISA)
  - ☑ Used by US Federal Government to define security controls

Agreement Types

Common agreements

- ☑ Memorandum of Understanding (MOU)
  - ☑ Both sides agree on the contents of the memorandum
  - ☑ Usually includes statements of confidentiality
  - ☑ Informal letter of intent; not a signed contract
- ☑ Memorandum of Agreement (MOA)
  - ☑ The next step above a MOU
  - ☑ Both sides agree to the objectives
  - ☑ A legal document, even without legal language
  - ☑ Unlike a contract, may not contain legally enforceable promises

Personnel Management

Personnel Management

Business policies

- ☑ Mandatory vacations - Rotate others through the job
  - ☑ The longer the vacation, the better chance to identify fraud
  - ☑ Especially important in high-security environments
- ☑ Job rotation
  - ☑ Keep people moving between responsibilities
  - ☑ No one person maintains control for long periods of time
- ☑ Separation of duties
  - ☑ Split knowledge
  - ☑ No one person has all of the details
  - ☑ Half of a safe combination
- ☑ Dual control
  - ☑ Two people must be present to perform a function
  - ☑ Two keys open a safe (or launch a missile)
- ☑ Clean desk policy
  - ☑ When you leave, nothing is on your desk
  - ☑ Limit the exposure of sensitive data to third-parties

Personnel Management

Background checks

- ☑ Background checks - Pre-employment screening
  - ☑ Verify the applicant’s claims
  - ☑ Discover criminal history, workers compensation claims, etc.
  - ☑ Legalities vary by country
- ☑ Adverse actions
  - ☑ An action that denies employment based on the background check
  - ☑ May require extensive documentation
  - ☑ Can also include existing employees

Personnel Management

Personnel security procedures

- ☑ NDA (Non-disclosure agreement)
  - ☑ Confidentiality agreement / Legal contract
  - ☑ Prevents the use and dissemination of confidential information
- ☑ Onboarding
  - ☑ Bring someone into the organization
  - ☑ Induction / Training - Usually a formal process
- ☑ Continuing education
  - ☑ Initial training isn’t enough
  - ☑ Security is constantly changing

Personnel Management

Acceptable use policies (AUP)

- ☑ What is acceptable use of company assets?
  - ☑ Detailed documentation
  - ☑ May be documented in the Rules of Behavior
- ☑ Covers many topics
  - ☑ Internet use, phones, computers, mobile devices, etc.
- ☑ Used by an organization to limit legal liability
  - ☑ If someone is dismissed, these are the well-documented reasons why

Personnel Management

Exit interviews

- ☑ Employee is leaving - Ask them a few questions first
- ☑ Information gathered can be used for improvements or changes
  - ☑ What are your reasons for leaving?
  - ☑ What did you like most? Least?
  - ☑ What could we have improved that would have caused you to stay?
- ☑ Very formal process and statistical record keeping
  - ☑ Useful for HR to compile and track

Role-based Awareness Training

Role-based Awareness Training

Role-based awareness training

- ☑ Before providing access, train your users
  - ☑ Detailed security requirements
- ☑ Specialized training
  - ☑ Each user role has unique security responsibilities
- ☑ Also applies to third-parties
  - ☑ Contractors, partners, suppliers
- ☑ Detailed documentation and records
  - ☑ Problems later can be severe for everyone

Role-based Awareness Training

Roles

- ☑ Data owner
  - ☑ Executive level manager, responsible for data security ultimately responsible for compliance
- ☑ System administrator
  - ☑ Administrator of the systems that enable the applications and data
  - ☑ May not necessarily be a user of the app or view the data
- ☑ System owner
  - ☑ Makes decisions about the overall operation of the app and data
  - ☑ Defines security policies and backup policies
  - ☑ Manages changes and updates

Role-based Awareness Training

User roles

- ☑ User
  - ☑ Application user
  - ☑ Has least privileged access to the application and data
- ☑ Privileged user
  - ☑ Additional application and data permissions
  - ☑ Area manager, report creation, user and password changes
- ☑ Executive user
  - ☑ Responsible for the overall operation of the application
  - ☑ High-level decision making for direction
  - ☑ Evaluates goals and makes decisions about future directions

General Security Policies

General Security Policies

Social media policies

- ☑ Balance the company reputation with employee participation
  - ☑ Social media use can be a great thing
- ☑ Extension of your code of conduct
  - ☑ Define requirements and expectations
  - ☑ Identification as an employee
  - ☑ Personal responsibility
- ☑ Confidential information
  - ☑ Public companies are legally bound
  - ☑ There’s a company spokesperson for public comments

General Security Policies

Personal email policies

- ☑ Qualify the use of email
  - ☑ Business use, no personal use
- ☑ Prohibit disruptive or offensive use
  - ☑ Avoid problems in the workplace
- ☑ Compliance issues
  - ☑ Some organizations are legally required to prohibit personal email
- ☑ The line becomes hazy when browser-based email is used
  - ☑ Is using Google Mail at work “personal email?”

Business Impact Analysis

Business Impact Analysis

Recovery

- Mean time to restore (MTTR)
  - Mean time to repair
- Mean time to failure (MTTF)
  - The expected lifetime of a product or system
- Mean time between failures (MTBF)
  - Predict the time between failures
- Recovery time objectives (RTO)
  - Get up and running quickly
  - Get back to a particular service level
- Recovery point objectives (RPO)
  - How much data loss is acceptable?
  - Bring the system back online; how far back does data go?

Business Impact Analysis

Calculating uptime and availability

- Expressed as a percentage over time
  - 99.999% availability
- "Availability" is a negotiated definition
  - Especially if it's part of your bonus

Availability	Annual Downtime (hh:mm:ss)
99.9999%	00:00:32
99.999%	00:05:15
99.99%	00:52:34
99.9%	08:45:36
99%	87:36:00

Mission-essential functions

- If a hurricane blew through, what functions would be essential to the organization?
  - That's where you start your analysis
  - These are broad business requirements
- What computing systems are required for these mission-essential business functions?
  - Identify the critical systems

Business Impact Analysis

Removing single points of failure

- A single event can ruin your day
  - Unless you make some plans
- Network configuration
  - Multiple devices (the "Noah's Ark" of networking)
- Facility / Utilities
  - Backup power, multiple cooling devices
- People / Location
  - A good hurricane can disrupt personnel travel
- There's no practical way to remove all points of failure
  - Money drives redundancy

Business Impact Analysis

Impact

- Life - The most important consideration
- Property - The risk to buildings and assets
- Safety - Some environments are too dangerous to work
- Finance - The resulting financial cost
- Reputation
  - An event can cause status or character problems

Business Impact Analysis

Privacy compliance

- Some compliance requires a public privacy statement
  - Gramm-Leach-Bliley Act (financial information), HIPAA (health care), etc.
- Privacy threshold analysis (PTA)
  - The first step in the compliance process
  - Identify business processes that are privacy-sensitive
  - Determines if a privacy impact assessment is required
- Privacy impact assessment (PIA)
  - Ensures compliance with privacy laws and regulations
  - What PII is collected, and why
  - How the PII data will be collected, used, and secured

Risk Assessment

Risk Assessment

Threat assessments

- Environmental threats
  - Tornado, hurricane, earthquake, severe weather
- Man-made threats
  - Internal threats are from employees, external threats are from outside the organizations

Risk Assessment

Quantitative risk calculation

- Likelihood - Annualized Rate of Occurrence (ARO)
  - How likely is it that a hurricane will hit? In Montana? In Florida?
- SLE (Single Loss Expectancy)
  - What is the monetary loss if a single event occurs?
  - Laptop stolen (asset value) = $1,000
- ALE (Annual Loss Expectancy)
  - ARO x SLE
  - Seven laptops stolen a year (ARO) x $1,000 (SLE) = $7,000
- The business impact can be more than monetary
  - Quantitative vs. qualitative

Risk Assessment

Evaluating risk

- Risk register
  - Every project has a plan, but also has risk
  - Identify and document the risk associated with each step
  - Apply possible solutions to the identified risks
  - Monitor the results
- Supply chain assessment
  - Get a product or service from supplier to customer
  - Evaluate coordination between groups
  - Identify areas of improvement
  - Asses the IT systems supporting the operation
  - Document the business process changes

Risk Assessment

Qualitative risk assessment

- Identify significant risk factors
  - Ask opinions about the significance
  - Display visually with traffic light grid or similar method

Risk Factor	Impact	ARO	Cost of Controls	Overall Risk
Legacy Windows Clients	🟡	🔴	🟡	🔴
Untrained Staff	🟢	🟡	🟢	🟡
No Anti-Virus Software	🟡	🔴	🟡	🔴

Business impact analysis

- What are your critical business functions?
  - Define the important business objectives
- What is impacted?
  - Loss of revenue, legal requirements, customer service
- How long will you be impacted?
  - You'll need personnel, equipment, resources
- What's the impact to the bottom line?
  - Is disaster recovery a good investment?

Risk Assessment

Testing for risk?

- Many servers contain sensitive data
  - Personal information, financial details, healthcare, etc.
- Running vulnerability and penetration tests can cause outages
  - You can't predict how a system will react
- Formal authorization is a best practice
  - Remove all legal liability from the testing
  - Vulnerability scanning is not very invasive
  - Penetration testing can install backdoors, perform DDoS attacks,
  - transfer sensitive data, and more

Risk Assessment

Risk response techniques

- Risk-avoidance
  - Stop participating in high-risk activity
- Transference
  - Buy some insurance
- Acceptance
  - A business decision; we'll take the risk!
- Mitigation
  - Decrease the risk level
  - Invest in security systems

Risk Assessment

Change management

- How to make a change
  - Upgrade software, change firewall configuration, modify switch ports
- One of the most common risks in the enterprise
  - Occurs very frequently
- Often overlooked or ignored
  - Did you feel that bite?
- Have clear policies
  - Frequency, duration, installation process, fallback procedures
- Sometimes extremely difficult to implement
  - It’s hard to change corporate culture

Incident Response Planning

Security incidents

Security incidents

- User clicks an email attachment and executes malware
  - Malware then communicates with external servers
- DDoS
  - Botnet attack
- Confidential information is stolen
  - Thief wants money or it goes public
- User installs peer-to-peer software and allows external access to internal servers

Security incidents

Examples of incidents categories

- External/removable media
  - Attack used removable media
- Attrition
  - A brute-force attack
- Web
  - Attack executed from a web site or web-based application
- Email
  - Attack executed from an email message or attachment
- Improper usage
  - Attack resulted from a violation of the Acceptable Use Policy
- Loss or theft of equipment
  - Laptop or mobile device stolen

Security incidents

Roles and responsibilities

- Incident response team
  - Specialized group, trained and tested
- IT security management
  - Corporate support
- Compliance officers
  - Intricate knowledge of compliance rules
- Technical staff
  - Your team in the trenches
- User community
  - They see everything

Security incidents

Incident notification

- Get your contact list together
  - There are a lot of people in the loop
- Corporate / Organization
- CIO / Head of Information Security / Internal Response Teams
- Internal non-IT
  - Human resources
  - Public affairs
  - Legal department
- External contacts
  - System owner, law enforcement
  - US-CERT (for U.S. Government agencies)

Security incidents

Cyber-incident response team (CIRT)

- Receives, reviews, and responds
  - A predefined group of professionals
- Determine what type of events require a CIRT response
  - A virus infection? Ransomware? DDoS?
- The CIRT may or may not be part of the organizational structure
  - Pulled together on an as-needed basis
- Focuses on incident handling
  - Incident response
  - Incident analysis
  - Incident reporting

Security incidents

Exercise

- Test yourselves before an actual event
  - Scheduled update sessions (annual, semi-annual, etc.)
- Use well-defined rules of engagement
  - Do not touch the production systems
- Very specific scenario
  - You probably have about four hours to do all of this
  - Table top exercise
- Evaluate response
  - Document and discuss

Incident Response Process

Incident Response Process

NIST SP800-61

- National Institute of Standards and Technology
  - NIST Special Publication 800-61
  - Computer Security Incident Handling Guide
- The incident response lifecycle:
  - Preparation
  - Detection and Analysis
  - Containment, Eradication, and Recovery
  - Post-incident Activity

Incident Response Process

Preparing for an incident

- Communication methods
  - Phones and contact information
- Incident handling hardware and software
  - Laptops, removable media, forensic software, digital cameras, etc.
- Incident analysis resources
  - Documentation, network diagrams, baselines, critical file hash values
- Incident mitigation software
  - Clean OS and application images
- Policies needed for incident handling
  - Everyone knows what to do

Incident Response Process

The challenge of detection

- Many different detection sources
  - Different levels of detail, different levels of perception
- A large amount of “volume”
  - Attacks are incoming all the time
  - How do you identify the legitimate threats?
- Incidents are almost always complex
  - Extensive knowledge needed

Incident Response Process

Incident indicators

- ☑ An attack is underway
  - ☑ Or an exploit is successful
- ☑ Buffer overflow attempt
  - ☑ Identified by an intrusion detection/prevention system
- ☑ Anti-virus software identifies malware
  - ☑ Deletes from OS and notifies administrator
- ☑ Host-based monitor detects a configuration change
  - ☑ Constantly monitors system files
- ☑ Network traffic flows deviate from the norm
  - ☑ Requires constant monitoring

Incident Response Process

Isolation and containment

- ☑ Generally a bad idea to let things run their course
  - ☑ An incident can spread quickly
  - ☑ It's your fault at that point
- ☑ Sandboxes
  - ☑ The attacker thinks they're on a real system
  - ☑ But they're not
- ☑ Isolation can be sometimes be problematic
  - ☑ Malware or infections can monitor connectivity
  - ☑ When connectivity is lost, everything could be deleted/encrypted/damaged

Incident Response Process

Recovery after an incident

- ☑ Get things back to normal
  - ☑ Remove the bad, keep the good
- ☑ Eradicate the bug
  - ☑ Remove malware
  - ☑ Disable breached user accounts
  - ☑ Fix vulnerabilities
- ☑ Recover the system
  - ☑ Restore from backups
  - ☑ Rebuild from scratch
  - ☑ Replace compromised files
  - ☑ Tighten down the perimeter

Incident Response Process

Reconstitution

- ☑ A phased approach
  - ☑ It's difficult to fix everything at once
- ☑ Recovery may take months
  - ☑ Large-scale incidents require a large amount of work
- ☑ The plan should be efficient
  - ☑ Start with quick, high-value security changes
    - □ Patches, firewall policy changes
- ☑ Later phases involve much "heavier lifting"
  - ☑ Infrastructure changes, large-scale security rollouts

Incident Response Process

Lessons learned

- ☑ Learn and improve
  - ☑ No system is perfect
- ☑ Post-incident meeting
  - ☑ Invite everyone affected by the incident
- ☑ Don't wait too long
  - ☑ Memories fade over time
  - ☑ Some recommendations can be applied to the next event

Incident Response Process

Answer the tough questions

- ☑ What happened, exactly?
  - ☑ Timestamp of the events
- ☑ How did your incident plans work?
  - ☑ Did the process operate successfully?
- ☑ What would you do differently next time?
  - ☑ Retrospective views provide context
- ☑ Which indicators would you watch next time?
  - ☑ Different precursors may give you better alerts

Gathering Forensics Data

Gathering Forensics Data

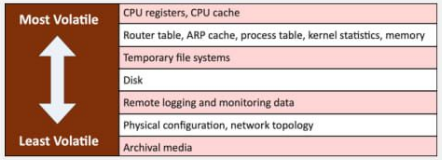
Forensic procedures

- ☑ Collect and protect information relating to an intrusion
  - ☑ Different data sources and protection mechanisms
- ☑ RFC 3227 - Guidelines for Evidence Collection and Archiving
  - ☑ A good set of best practices
- ☑ Standard digital forensic process
  - ☑ Acquisition, analysis, and reporting
- ☑ Must be detail oriented - Take extensive notes

Gathering Forensics Data

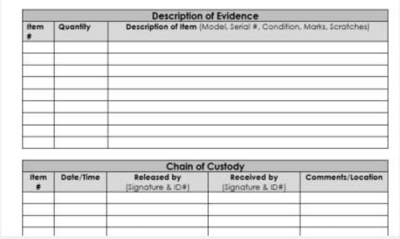
Order of volatility

- ☑ How long does data stick around?
  - ☑ Some media is much more volatile than others
  - ☑ Gather data in order from the most volatile to less volatile


Most Volatile
Least Volatile
CPU registers, CPU cache
Router table, ARP cache, process table, kernel statistics, memory
Temporary file systems
Disk
Remote logging and monitoring data
Physical configuration, network topology
Archival media

Chain of custody

- ☑ Control evidence - Maintain integrity
- ☑ Everyone who contacts the evidence
  - ☑ Avoid tampering - Use hashes
- ☑ Label and catalog everything
  - ☑ Seal and store



Description of Evidence

Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody

Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

Gathering Forensics Data

Legal hold

- ☑ A legal technique to preserve relevant information
  - ☑ Prepare for impending litigation
  - ☑ Initiated by legal counsel
- ☑ Hold notification
  - ☑ Records custodians are instructed to preserve data
- ☑ Separate repository for electronically stored information (ESI)
  - ☑ Many different data sources and types
  - ☑ Unique workflow and retention requirements
- ☑ Ongoing preservation
  - ☑ Once notified, there's an obligation to preserve data

Gathering Forensics Data

Capture system image

- ☑ Copy the contents of a disk - bit-for-bit, byte-for-byte
  - ☑ Get every morsel of information
- ☑ Software imaging tools - Use a bootable device
- ☑ Remove the physical drive
  - ☑ Use a hardware write-blocker
- ☑ Get the backup tapes
  - ☑ Some of this work may have been done for you

Gathering Forensics Data

Network traffic and logs

- ☑ Traffic logs
  - ☑ Very common
  - ☑ Firewalls log a lot of information
  - ☑ Switches and routers don't usually log user-level information
- ☑ Intrusion Detection/Prevention Systems
  - ☑ Log usual traffic patterns
- ☑ Raw network traffic data
  - ☑ Stream-to-disk
  - ☑ An exact recording of network communication
  - ☑ Rebuild images, email messages, browser sessions, file transfers

Gathering Forensics Data

Capture video

- ☑ A moving record of the event
  - ☑ Gathers information external to the computer and network
- ☑ Captures the status of the screen and other volatile information
  - ☑ Today's mobile video devices are remarkable
- ☑ Don't forget security cameras and your phone
- ☑ The video content must also be archived
  - ☑ May have some of the most important record of information

Gathering Forensics Data

Recording time offsets

- ☑ Windows: 64-bit time stamp
  - ☑ Number of 100-nanosecond intervals since
    - □ This stops working in 58,000 years
- ☑ Unix: 32-bit time stamp
  - ☑ Number of seconds since January 1, 1970 00:00:00 GMT
    - □ This stops working on Tuesday, January 19, 2038 at 3:14:07 GMT
- ☑ Different file systems store timestamps differently
  - ☑ FAT: Time is stored in local time
  - ☑ NTFS: Time is stored in GMT
- ☑ Record the time offset from the operating system
  - ☑ The Windows Registry
  - ☑ Many different values (daylight saving time, time change information, etc.)

Gathering Forensics Data

Take hashes

- ☑ How can you ensure that there's no tampering?
  - ☑ Use a digital hash
- ☑ MD5 (Message Digest 5)
  - ☑ 128 bits, displayed as hexadecimal
  - ☑ Chance of duplication is one in 2128 (230 billion billion billion billion)
- ☑ CRC (Cyclical Redundancy Check)
  - ☑ 32 bits, displayed as hexadecimal
  - ☑ One in 232 (4,294,967,296)
- ☑ Create an MD5 hash for an image or files
  - ☑ Data can be verified at any time

Gathering Forensics Data

Screenshots

- ☑ Capture the state of the screen
  - ☑ Difficult to reproduce, even with a disk image
- ☑ External capture - Use digital camera or phone
- ☑ Internal capture - PrintScreen, third-party utility

Witnesses

- ☑ Who might have seen this?
  - ☑ You won't know until you ask
- ☑ Interview and document
  - ☑ These folks might not be around later
- ☑ Not all witness statements are 100% accurate
  - ☑ Humans are fallible

Using Forensics Data

Using Forensics Data

Preservation

- ☑ There will be a lot of data
  - ☑ You need to keep it all
- ☑ Important for the current investigation
  - ☑ Immediate need to sift through the evidence
- ☑ There may be a future investigation
  - ☑ Or revisit the existing event
- ☑ New items of interest may be discovered
  - ☑ You'll need the data to explore these new items

Using Forensics Data

Recovery

- ☑ Strategic intelligence
  - ☑ Collect and process information
  - ☑ What important information did you find?
  - ☑ Base security policy changes on this intelligence
- ☑ Counterintelligence gathering
  - ☑ What do we know about the attacker?
  - ☑ Learn as much as you can about the attacker's habits
- ☑ Active logging
  - ☑ Log everything, everywhere
  - ☑ Track every step the attacker takes

Using Forensics Data

Track man hours and expenses

- ☑ Some incidents can use massive resources
  - ☑ All at once
  - ☑ Over a long period
- ☑ May have an impact on the bottom line
  - ☑ Can be wide ranging
- ☑ May be required for restitution
  - ☑ Be as accurate as possible

CSF 434/534: Advanced Network and System Security

Week 10 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes