2.6.5 Incident Response Facts

A *security incident* is an event or series of events that are a result of a security policy violation that has adverse effects on a company's ability to proceed with normal business. Security incidents include the following:

- Employee errors
- Unauthorized acts by employees
- Insider attacks
- External intrusion attempts
- Virus and harmful code attacks
- Unethical gathering of competitive information

Incident response is the action taken to deal with an incident during and after the incident. Prior planning helps people know what to do when a security incident occurs. Incident response plans should:

- Define what is considered an incident.
- Identify who should handle the response to the incident. This person is designated as the *first responder*.
- Describe what action should be taken when an incident is detected.
- Provide a detailed outline of steps to be taken to handle an incident both efficiently and effectively, while mitigating its effects.
- Explain how and to whom an incident should be reported.
- Explain when management should be notified of the incident and also outline ways to ensure that management is well-informed.
- Be legally reviewed and approved.
- Be fully supported by senior management and administration with appropriate funding and resources such as camera equipment, forensic equipment, redundant storage, standby systems, and backup services.

The incident handling plan should be known to all members of the company in leadership positions. At least one member of every department should be trained to recognize abnormal activities, suspicious behavior, unauthorized code activity, and irregular patterns in employee conduct. In addition, employees should be trained to report security incidents or suspicious activity immediately to the proper company staff members or directly to the first responder. Once an incident has been discovered, the following actions should occur:

1. Recognize and declare the event.
2. Preserve any evidence that may be used in an investigation.
3. Contact the first responder.

In some organizations, the first responder may be a Computer Incident Response Team (CIRT), a group of in-house experts that are trained to quickly respond to a crisis computer event. A CIRT should have representation from any department that may be affected by an incident (representation from the Human Resources and Legal departments should always be included). A CIRT should also consist of members with computer network skills, evidence handling training, and forensic skills.

In responding to security incidents, you will often work closely with law enforcement agencies and third-party forensic responders. However, even if these entities perform the bulk of work in investigating the case and mitigating damage to your system, you should be familiar with the incident response process from beginning to end. The following table provides more information on responding to security incidents:

Concern	Description
Incident Response Process	The security incident response process includes the following steps: ▪ *Preparation*. As described above, a detailed incident response plan must be in place long before a security incident occurs. ▪ *Identification*. Before any action can be taken to contain the problem, it must be clearly identified. What security policy was violated and what is the scope of the attack? ▪ *Containment*. After identifying the problem, the next step is to take actions to stop the attack and contain or limit the damage. For example, if the attack involves a computer system attached to the network, the first step might be to disconnect the system from the network. Although you want to preserve as much information as possible to assist in later investigations, it might be better to stop the attack, even if doing so alerts the attacker or results in the loss of evidence regarding the attack. In the case of a virus, isolate any systems that may be able to spread the virus to additional systems. ▪ *Eradication*. The next step is to eradicate the cause of the incident, while carefully preserving evidence that may be used in a criminal investigation. ▪ *Recovery*. After isolating and removing whatever caused the security incident, the recovery stage includes repairing any damage to the system. ▪ *Lessons Learned*. The final step includes documenting the investigation, notifying all affected parties, and implementing countermeasures and processes to reduce the likelihood of a future attack.
Response Timeframes	Responding to a security incident will be similar to responding to any other type of incident. ▪ Short-term (triage) actions focus on stopping the attack, mitigating its effects, and restoring basic functionality. ▪ Mid-term (action/reaction) actions focus on restoring operations to a normal state. ▪ Long-term (follow up) actions include implementing additional countermeasures and processes to reduce the likelihood of a future attack.

First Responder	The first responder:
	- May be a dedicated member of the security response team.
	- Has the following goals:
	  - Contain the damage (or incident) as much as possible.
	  - Do not damage any evidence.
	- Initiates an escalation procedure to ensure that the right people are informed and the right people are brought on the incident site.
	- Initiates the documentation of the incident.
	- Should have access to documentation for all aspects of the affected system.
	- Should maintain a thumb drive with commonly used tools and utilities.

Crime Scene Evidence	Preservation of the crime scene and evidence is critical. - Allow only authorized personnel trained in incident response to touch compromised systems. - After securing the area, gather and preserve evidence before attempting to restore systems or bring them back into production. - When investigating the crime, review and make a backup of all logs, video-tapes, audit trails, surveillance, etc. Make sure that all possible measures are taken to prevent contamination or loss of key evidence.
Damage Assessment	One of your first steps should be to perform an initial damage assessment. Notify senior management of the damage and determine who should respond to and investigate the incident. Carefully consider whether or not you should use in-house skills to accomplish a full investigation of the crime. Using in-house skills can help the company maintain greater control over the crime scene and the investigation. Outside professional support might be necessary for certain cases but usually involves a lack of privacy and added expense.
Internet Connectivity	Internet connectivity may not be possible through the standard network connection. A Web-enabled smart phone or tablet device that will allow internet access for sending notification e-mails and accessing information for problem resolution should be available.
Working with Law Enforcement	Keep in mind that it may be a crime not to report an incident to the proper authorities. If necessary, notify police or other authorities. Be aware that once you contact the police, the investigation is completely out of your control. The decision to notify the police should be made solely by senior management. The police should be notified in the following order: - Contact the local police first. - Contact the FBI if it is a nationwide or intrastate crime. - Contact the Secret Service if it is an International crime. If an employee is acting under the instruction of a police officer, all police search and seizure laws apply to the employee. If the employee is acting as a private citizen, search and seizure policies typically do not apply.
Government Requirements	Government organizations may have very specific reporting requirements. For example, the United States federal government uses the following incident reporting requirements for different levels of incidents: - A *Category 1* event occurs when an individual gains unauthorized access to a federal system and should be reported within one hour of detection. - A *Category 2* event occurs when a denial of service (DoS) attack is under way and should be reported within two hours of detection. - A *Category 3* event occurs when a malware infection occurs on a federal system and should be reported within one hour of detection. - A *Category 4* event occurs when a federal employee violates acceptable use policies and should be reported weekly. - A *Category 5* event occurs when a reconnaissance scan of a federal system is detected and should be reported within one hour.
The Media	Avoid all contact with media or outside influences in any way. Interact only with the first responder and any other professional groups assigned to the investigation. Only designated personnel should be authorized to contact the media.
Crime Suspects	Identify primary suspects. Potential suspects have motive, opportunity, and means (the ability to commit the crime). When carrying out an investigation, it is important to determine the *Method of Operation* (MO) of each suspect. Defining a person's motive (e.g. vengeance, profit, attention) helps the investigators to develop an understanding of who may have been capable of the crime. A suspect's method of operation usually has three purposes: to assist in escaping, to ensure the crime's success, and to protect the attacker's identity. Assessing each suspect's MO can lead to discoveries that may be indicative of: - The amount of planning necessary for the crime to be executed. - Access to surveillance or intelligence. - The method in which the attack was executed. - Any precautionary acts that may have been used.

When working with computer systems, use special computer forensic tools to analyze the system. Investigations can be performed in the following ways:

- A *live analysis* examines an active (running) computer system to analyze the live network connection, memory contents, and running programs.
- A *dead analysis* examines data at rest, such as analyzing hard drive contents.
- *Big data analysis* can be used to identify anomalies that led up to the attack. Big data is the combination of all types of data used in the organization, including text, audio, video, and log files.

The following table describes procedures you should use when collecting and analyzing computer evidence:

Procedure	Description
Taking Photographs	Before touching the computer, document and photograph the entire scene of the crime including the current state of the computer screen. A traditional camera is preferred over a digital camera to avoid charges that an image was digitally altered.

Collecting Data	Do not turn off the computer until the necessary evidence has been collected.
	- Some data might be lost when the computer is turned off.
	  - *Volatile* data is any data that is stored in memory that will be lost when the computer is powered off or loses power.
	  - *Persistent* data resides on the system's hard drives, USB drives, optical media, and other external hard drives.
	- When collecting forensic data, follow the order of volatility. Gather the most volatile data first and leave more persistent data for later. The following list ranks data from most to least volatile:
	1. Contents of the processor's cache and data registers
	2. Contents of RAM and data stored on network devices such as routing and process tables
	3. Temporary file system data stored in local memory
	4. Data stored on disk
	5. Remote logging and monitoring data
	6. Network topology and physical configuration of the system
	7. Achival media
	- If it is necessary to isolate a system to stop or prevent future attacks, disconnect the system from the network rather than shutting it down (if possible). In some situations, you may be able to connect the system to a quarantine network to perform a forensic investigation.
	- Turning off the system might be the only practical method to prevent further damage and should be done if necessary, even if it results in the loss of potential evidence.

Seeking Investigative Help	Assess the situation to determine whether you have the expertise to conduct further investigations, or whether you need to call in additional help.
Analyzing Data	Analyze data in order from most volatile to least volatile: 1. Registers and caches 2. RAM 3. Dynamic memory and temporary file systems 4. Hard disk data 5. Off-site logging and monitoring data 6. Archived media
Saving Memory Contents	Save the contents of memory by taking one of the following actions: - Save and extract the page file. - Do a complete memory dump to save the contents of physical RAM. The page file will be lost but the physical memory will be preserved.
Analyzing Hard Disks	Clone or image hard disks. - To protect or ensure the integrity of collected digital evidence, create a checksum using a bit-level hashing algorithm. In the future, the same hashing algorithm can be used to create another checksum. If the two checksums are identical, this proves that the media was not altered (and that the copy is an exact copy of the original). - Never analyze the original data. Make several copies for analysis to preserve the original. Bit-level cloning is the best method for duplicating hard drives for forensic investigative purposes. - Make sure to use only forensic tools for which you can provide proof of official licensing and authorization in court. - Make a hash of any copies you make. This hash proves that your copy matches the original. - Archive the original system or data for later investigations and comparisons to your copy.
Hidden Files	In addition to looking for obvious evidence on computer systems (such as saved files), use special forensic tools to check for deleted files, files hidden in slack (empty) space, or data hidden in normal files through the use of steganography.

Log Files	For some investigations, you might need to review archived log files or data in backups to look for additional evidence. Be sure to design your backup strategy with not only recovery but also investigation and evidence preservation in mind.
Co-Mingling Data	Sometimes evidence is found on a corporate system that is not otherwise violated. This is known as *co-mingling*. Evidential data should be extracted from the corporate system with great care to maintain its integrity and also the safety of the corporate system.
Tracking Expenses	Track man hours and expenses for each incident. This may be necessary to calculate a total damage estimation and possibly restitution.
Analyzing Network Traffic	You may need to capture and analyze network traffic to understand the incident. This may include: 1. Identifying suspicious network sessions and packets 2. Replaying or reconstructing sessions and packets 3. Interpreting the results
Time Offset	The *time offset* is the difference in system time that the machines use compared to the actual time. You should record the time offset for each machine involved with the incident to ensure accurate and sequential date and time stamps for collected data.
Data Analysis Utilities	Utilities available to help in the analysis of the evidence include: ▪ SANS Investigative Forensics Toolkit ▪ EnCase ▪ FTK ▪ The Coroner's Toolkit ▪ COFEE
Restoring Services	Repair any damage created by the incident and restore services only after the above procedures are complete.
Reporting Findings	Once the analysis is complete, the findings are reported. The report should be well written, possibly with the assistance of an attorney. Specifically, the report must be self-contained and describe the incident, the response, and the findings. Be sure to include a section relating the lessons learned from the incident and how they should influence your organization's security posture. You should also include the hours and expenses involved in responding to the incident.