

Flexible Instruction Day Assignment #4

A Review of Incident Response & Regulated Data

This material can be found in section 1008 of the State Tasklist and is part of the exam objectives of the CompTIA A+, Network+ & Security + certifications.

In this packet we will cover the basics of incident response and look at common regulations for data.

What is an incident and how do we know if we have had one?

A security incident is any event that can negatively impact an organization's data or systems. This would include someone stealing or destroying data, someone gaining access to restricted content, someone trying to gain unauthorized access to a system or area, and there are many more examples.

An organization should have detailed plans (security policies, incident response plans, etc.) of who will respond and what will be done in the case of a security incident. Companies will make sure to test these plans and update date them to make sure that the security concerns are being addressed.

How do they know an incident has occurred?

Companies want to detect and react to a security incident as quickly as possible so damage can be minimized, and systems can be operational again. The best approach is **proactive** because you can prepare for and prevent incidents before they happen. This is accomplished by testing the security systems to look for flaws (and fixing them) as well as keeping track of security threat patterns and developments. Organizations also **actively** monitor their systems with devices and programs like IDS (intrusion detection systems), firewalls, network monitors, packet sniffers, malware detection software, etc. This allows the organization to detect and respond to incidents as they are occurring. These active systems are not only set up to alert you that an incident is happening, they can also be set to automatically respond. Sometimes organizations discover security incidents when they are not actively looking for them (called

passive detection). This may happen when a technician discovers suspicious activity while looking through log files or while they are performing maintenance on a system/computer.

What happens when an incident is detected?

Organizations have detailed and tested incident response plans/policies. This plan outlines what will be done, by who, and when. This way, the response is done in a consistent, efficient, and secure manner. First responders would start the process, but the actual investigation would be handled by a forensics team. Other response/security team members would be in charge of fixing the damage/implementing changes, etc. The first steps in the plan are designed to stop the threat and to preserve evidence; this would be done by a first responder.

The **first responder** will secure and record the scene by collecting and tagging evidence, interviewing witnesses, recording dates, times, locations, names, etc. The first responder will preserve and collect volatile evidence (from memory, hard drives, etc..) and will contact the other needed people (security/response team people, law enforcement, etc.).

If the first responder does a bad job, evidence could be lost or inadmissible and the extent of the damage could be much worse. The term **Chain of Custody** refers to the detailed procedures and documentation that needs to be followed for the evidence to be allowed in a court of law. If the chain of custody is not followed, someone could claim that the evidence was planted or altered, and you would have no proof that it wasn't. Without a predefined plan/the chain of custody, the first responder would not know what to do, who to call, how it is to be done and in what order.

Once things are secured and the initial evidence is collected by the first responders, the rest of the response team would be notified, and the forensics team would be in place to collect further evidence and run the investigation. As we mentioned earlier, other security/response team members would be in charge of fixing the affected system/recovery.

The last step of the incident response involves the participants meeting and reviewing what was done to look for improvements and to see what could be done to prevent the incident from happening again. This meeting/review is sometimes called a Post-Mortem or hot-wash.

Regulated Data

At this point, most people are aware of the seriousness of protecting data. You may be careful on your end but who is making sure that companies/organizations are keeping your information safe; who is making them accountable? Lets look at some of the more common Laws & Regulations that are currently in place.

Personal information is typically categorized as **personal government-issued information** (Social Security#, Drivers license#, etc.) or **personally identifiable information (PII)** (address, credit info, student records, etc.). PII is regulated by **FERPA**(Family Educational Rights and Privacy Act- regulates how schools keep student info.) **CCPA**(California Consumer Privacy Act- gives Californians control over the information business collect about them).

Healthcare Information is regulated by **HIPAA** (Health Insurance Portability and Accountability Act). HIPPA defines rules on how health care information must be secured/protected (how it must be stored, who can have access to what, etc.).

Financial Information is largely protected by the **PCI DSS** (Payment Card Industry Data Security Standards) **GLBA** (Gramm-Leach-Bliley Act) & **SOX** (Sarbanes-Oxley Act). PCI DSS protects payment card data (credit/debit cards, etc.) by make requirements as to how organizations protect your card information (how it is stored, encrypted, restricting access, etc.). GLBA uses the Federal Trade Commission to enforce rules about how organizations who deal with investments, loans or insurance, must safeguard customer information. Sox regulates how publicly traded companies maintain financial records and secure financial data.

What happens if you fail to follow these laws & regulations? The penalty will of course depend to the severity of the violation, but it can range from jail to fines and suspension of your ability to practice/run your business.