# Incident Response

## Incident Response

When you've had a data breach, you may need forensic analysis to analyze the attack. This analysis usually involves extensive evidence gathering. This reading covers some considerations for protecting the integrity of your forensic evidence and avoiding complications or issues related to how you handle evidence.

### Regulated data

It's important to consider the type of data involved in an incident. Many types of data are subject to government regulations that require you to take extra care when handling it. Here are some examples you're likely to encounter as an IT support specialist.

1. **Protected Health Information:** This information is regulated by the Health Insurance Portability and Accountability Act (HIPAA). It is personally identifiable health information that relates to:

- Past, present, or future physical or mental health or condition of an individual
- Administration of health care to the individual by a covered provider (for example, a hospital or doctor)
- Past, present, or future payment for the provision of health care to the individual

2. **Credit Card or Payment Card Industry (PCI) Information:** This is information related to credit, debit, or other payment cards. PCI data is governed by the Payment Card Industry Data Security Standard (PCI DSS), a global information security standard designed to prevent fraud through increased control of credit card data.

3. **Personally Identifiable Information (PII):** PII is a category of sensitive information associated with a person. Examples include addresses, Social Security Numbers, or similar personal ID numbers.

4. **Federal Information Security Management Act (FISMA) compliance:** FISMA requires federal agencies and those providing services on their behalf to develop, document, and implement specific IT security programs and to store data on U.S. soil. For example, organizations like NASA, the National Institutes of Health, the Department of Veteran Affairs—and any contractors processing or storing data for them—need to comply with FISMA.

5. **Export Administration Regulations (EAR) compliance:** EAR is a set of U.S. government regulations administered by the U.S. Department of Commerce's Bureau of Industry and Security (BIS). These regulations govern the export and re-export of commercial and dual-use goods, software, and technology. Dual-use goods are items that can be used both for civilian and military applications. These goods are heavily regulated because they can be classified for civilian use and then transformed for military purposes.

### Digital rights management (DRM)

Digital Rights Management (DRM) technologies can help ensure data regulations compliance. DRM technology comes in the form of either software or hardware solutions. Both options allow content creators to prevent deliberate piracy and unauthorized usage. DRM often involves using codes that prohibit content copying or limit the number of devices that can access a product. Content creators can also use DRM applications to restrict what users can do with their material. They can encrypt digital media so only someone with the decryption key can access it. This gives content creators and copyright holders a way to:

- **Restrict users** from editing, saving, sharing, printing, or taking screenshots of content or products
- **Set expiration dates** on media to prevent access beyond that date or limit the number of times users can access the media
- **Limit access** to specific devices, Internet Protocol (IP) addresses, or locations, such as limiting content to people in a specific country

Organizations can use these DRM capabilities to protect sensitive data. DRM enables organizations to track who has viewed files, control access, and manage how people use the files. It also prevents files from being altered, duplicated, saved, or printed. DRM can help organizations comply with data protection regulations.

### End User Licensing Agreement (EULA)

End User Licensing Agreements (EULAs) are similar to DRM in specifying certain rights and restrictions that apply to the software. You often encounter EULA statements when installing a software package, accessing a website, sharing a file, or downloading content. A EULA is usually considered a legally binding agreement between the owner of a product (e.g., a software publisher) and the product's end-user. The EULA specifies the rights and restrictions that apply to the software, and it's usually presented to users during installation or setup of the software. You can't complete an installation (or access, share, or download data) until you agree to the terms written in the EULA statement.

Unlike DRM restrictions, EULAs are only valid if you agree to it (i.e., you check a box or click the 'I Agree' button). DRM restrictions don't require your agreement—or rely on you to keep that agreement. DRMs are built into the product they protect, making it easier for content creators to ensure users do not violate restrictions.

### Chain of custody

"Chain of custody" refers to a process that tracks evidence movement through its collection, safeguarding, and analysis lifecycle. Maintaining the chain of custody makes it difficult for someone to argue that the evidence was tampered with or mishandled. Your chain of custody documentation should answer the following questions. Documentation for these questions must be maintained and filed in a secure location for current and future reference.

- Who collected the evidence? Evidence can include the afflicted or used devices, media, and associated peripherals.
- How was the evidence collected, and where was it located?
- Who seized and possessed the evidence?
- How was the evidence stored and protected in storage? The procedures involved in storing and protecting evidence are called evidence-custodian procedures.
- Who took the evidence out of storage and why? Ongoing documentation of the names of individuals who check out evidence and why must be kept.

When a data breach occurs, forensic analysis usually involves taking an image of the disk. This makes a virtual copy of the hard drive. The copy lets an investigator analyze the disk's contents without modifying or altering the original files. An alteration compromises the integrity of the evidence. This kind of compromised integrity is what you want to avoid when performing forensic investigations.

### Key takeaways:

Incident handling requires careful attention and documentation during an incident investigation's analysis and response phases.

- Be familiar with what types of regulated data may be on your systems and ensure proper procedures are in place to ensure your organization's compliance.
- DRM technologies can be beneficial for safeguarding business-critical documents or sensitive information and helping organizations comply with data protection regulations.
- When incident analysis involves the collection of forensic evidence, you must thoroughly document the chain of custody.

**Mark as completed**