

Control Essentials

Volume II, Issue I

April 2006

Page 1/2

Enterprise Risk Management provides the following services:

- Information Security Design and Implementation
- Risk Assessments
- Vulnerability Assessments
- Penetration Testing Studies
- Security Remediation
- Internal Information Systems Audits
- Application Control and Security Services
- Business Continuity Plan (BCP) Services
- Attestation and Assurance
 - SAS-70
 - Others
- Compliance with Federal Laws and Regulations
 - Sarbanes - Oxley
 - GLBA
 - HIPAA
- Forensic Examinations

Computer Forensics

What is Computer Forensics?

The skills of computer forensics are critical for an organization to be able to determine whether electronic devices have been utilized for illegal, unauthorized, or unusual activities, and to collect evidence in a way that it will be admissible in court. Computer forensics is the process by which digital evidence is identified, preserved, analyzed and presented. Forensic investigations generally include the following five phases:

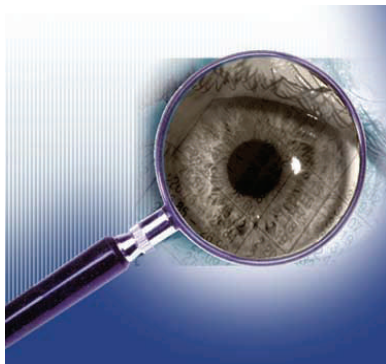
Verification

The purpose of this phase is to determine whether an incident requires a forensic investigation or not. The trigger event for this phase is the detection of suspicious activity. As an organization, it is really important to have the possible events that could trigger an investigation explicitly defined.

System Description

Once an event has been verified and an investigation has been triggered, it is necessary to determine the devices that need to be included in the scope of the investigation. This information is essential because it will affect the manner in which the investigation will be executed. For example, the scope of the investigation may be limited to one laptop or it may involve an entire network.

This phase determines the answers to the famous questions "Should I unplug the machine or not?" and "Should I shutdown or power-off the machine?" The answer to these questions will vary depending on the type of investigation being conducted. Every time one of these questions arises what must be considered is how much information will be lost and if that information is relevant to the investigation.



Evidence Collection

Once the devices are identified, it is time to start collecting the evidence. Evidence can be defined as everything that can prove or disprove a fact. Generally, the "best evidence rule" demands that the original copy of any document, photograph or recording be used as evidence at trial, rather than a duplicate copy. A duplicate copy may be allowed if it can be properly authenticated as a true and accurate copy.

As the focus is on volatile information, due to its nature, the likelihood of losing some of this evidence significantly increases. Therefore, extreme care must be taken to ensure minimal loss of information and preservation of its quality.

Computer Forensics (continued...)

The bottom line is to ensure that the evidence has not been corrupted. Thanks to modern technology, there are currently many tools that allow investigators to keep the integrity of the evidence.

Analysis

This is the phase where the real investigation takes place. So far, the existence of a forensic case has been determined, the devices involved in the case have been identified and evidence has been gathered. In order to conduct the analysis, it is necessary to have an exact copy of the best evidence. As a rule of thumb, the analysis will not be performed on original evidence. The analysis can be divided into two steps:

The Creation of the Timeline - The timeline provides a foundation for the investigation, as the investigation will revolve around it.

The Recovery of the Data - Data recovery is the key function of forensics. This process includes recovering deleted files, images and e-mails.

As in the previous phase, the information gathered should be preserved and its integrity must be maintained.



Reporting

Based on the analysis performed and the information gathered, a report has to be generated. This report should include the objective of the case, the devices under investigation, an explanation of how the evidence was obtained and preserved, an explanation about the analysis process and the conclusion. Many investigators overlook this phase because they think that people understand technology. However, in a court of law or in your own organization, this report must be comprehensive enough to be utilized by anyone. Therefore, it is important to make sure that it is clear and understandable.

Summary

In short, computer forensics is needed to identify, preserve, analyze and present digital evidence. Since the evidence is digital, its preservation is one of the key factors in the success of an investigation. In addition, the analysis of the evidence must be reported clearly, so that this technical evidence can be effectively used for the benefit of the affected organization.