

# Control Essentials

Volume II, Issue X

October 2007

## Business Consulting

- Regulatory Support
  - Policies and Procedures
  - Regulatory Compliance
    - Sarbanes-Oxley
    - GLBA
    - HIPAA
    - BSA
  - PCI (Payment Card Industry) Security Audit
  - Information System Audit Outsourcing
- Enterprise Support
  - Business Continuity Planning
  - Attestation and Assurance
    - SAS-70
  - E - Discovery
  - Forensic Examinations
  - Security Remediation

## Technology Consulting

- Application Security
  - Application Security Assessment
  - Application Penetration Test
  - Web Application Security Assessment
  - Web Application Penetration Test
- Network Security
  - Risk Assessment
  - Vulnerability Assessment
  - Penetration Testing
    - Internal
    - External
    - Social Engineering
    - War Dialing
    - War Driving
    - Blue Snarfing
  - Wireless Security Assessment
  - Information System Security Audit
  - Information System Control Audit
  - Network Architecture Design and Assessment
  - Physical Security Assessment
  - Log Analysis

## Computer Forensics

Computers have changed many aspects of our lives. Today almost all businesses and professionals depend on computers.

Computers have also changed the nature of the evidence that is needed for legal proceedings. Almost everything, from financial statements to blueprints to voice recordings, are now stored in digital format. What would have been correspondence and phone conversations in the past are now emails.

Because so much is stored in digital form, computer forensics has become essential in an increasing number of circumstances. "Forensics" refers to the application of science to address questions related to legal matters. However, because computers are an essential part of business and security, computer forensics skills are used in examinations conducted when no legal proceedings are even yet contemplated. For example, computer forensics is often used in corporate internal investigations, or in response to a security incident.

"Computer forensics" refers to examinations of computers and networks applying knowledge and skills related to computer science and related to the proper gathering and analysis of evidence. In many circumstances, businesses find that there is some electronic data that a forensic expert must preserve, retrieve, and analyze in connection with an investigation. Also, if the matter goes to court, a forensic expert is often needed to testify about the integrity of the evidence and the conclusions reached as a result of forensic analysis.

### A Structured Methodology

Computer Forensics requires a detailed, methodical process. A proper methodology includes the following phases:

#### 1. Scope Definition

The first step in a forensic investigation is to obtain background information about the events that have already taken place and about the environment that is being considered for the investigation. This is necessary to define the scope of the investigation.

The scope of the investigation could range from a single laptop computer to a complete network. In cases where an entire network needs to be investigated, the next step would be to map and identify all the machines and devices in the network environment. This task may be further complicated if there are rogue devices on the network.

The scope definition will indicate the engagement's goals and search criteria. The scope of the engagement will also affect the results that can be expected from a particular forensic investigation.



## 2. Evidence Acquisition

Evidence collection involves a number of steps: collecting the original evidence; identifying the collected evidence; documenting and preserving the collected evidence; and securely storing and safeguarding the evidence.

The collection of evidence must be done in a way that preserves “the chain of custody” of the evidence. This means that the expert will maintain proof (paper and electronic records) showing that there has been constant control of the evidence.

This is critical because for evidence to be admitted in court legal rules require proof that the evidence has not been altered. By proving constant, secure control of the evidence, an expert can establish that no one altered it. Another way that experts maintain proof of the integrity of the digital evidence is by maintaining the “hash value” of the data that was imaged. The “hash value” is like a mini-snapshot of the evidence. If, at a later date, a “hash value” of the imaged data is taken again, this mini-snapshot would need to be the same as the one taken when the data was first imaged.

## 3. Evidence Documentation

Another important part of a proper forensic investigation is documentation. In addition to documenting the chain of custody, forensic experts will maintain detailed documentation of all the steps performed and all the commands executed. This documentation is not only important for maintaining the integrity of the evidence, but is also indispensable for accurate testimony in court.

The documentation that is maintained relates to both physical and logical evidence. Examples of physical evidence are the serial number, cylinder heads, and physical markings of a hard drive. Examples of logical evidence are the number and size of partitions, the file structure, and files within a hard drive.

## 4. Examination Plan

A forensic expert’s examination plan will generally include: a statement of the examination goal; the criteria that will be used to select tools; a description of procedures that will be used; the criteria that will be used to select or reject data; and the format that will be used for the outputs.

When designing the examination plan, the forensic expert determines where and how to look for certain items that fit selected criteria. Examples of criteria include but are not limited to application data, names, strings, file types, and dates. The examiner will also select the tools and the data harvesting techniques that will be utilized for the particular case. An efficient examiner will choose tools that will help him or her to look for the items that fit the criteria for the search with minimum data burden. The examiner will also plan the data reduction, identification, indexing and reconstruction functions.

The examination plan will also include a process for comparing the results to the original goals so that the examination plan can be revised as necessary.

## 5. Examination Execution

The execution of the examination will follow the examination plan. The execution will include the following steps:

**Data recovery** - the steps taken to find any latent information and to restore its context.

**Data reduction** - the elimination of any non-significant data.

**Data identification** - finding the data that meets the scope criteria.

**Data search** - performing relative string searches on identified data sets.

**Reconstruction** - reconstruction of key elements, such as actual timeline retrieval and analysis, any log file correlations, and any additional layer analysis.

**Content analysis** - analysis of any other content, such as images and multimedia.



The analysis phase is carried out on an identical copy or “image” of the digital evidence. A “hash value” of the image is used to verify that the image is indeed an identical copy of the original evidence. This process is essential so that the original evidence remains intact. At the end of the analysis stage, the forensic expert attempts to create a timeline of events that will aid the investigation.

## **6. Reporting**

The results of the examination will be summarized in a formal report. The report will describe the significant steps that were taken and the results. The report may also include examples of the data found. Additionally, the report will include the expert's conclusions and/or expert opinions. When legal proceedings are involved, the report will be disclosed to the opposing party, and the report will be the basis for the expert's testimony at a deposition or in court.

### **Conclusion**

Computer forensic examinations have become increasingly common. Businesses use them in internal investigations of many matters including security breaches. They are also used when legal matters arise because almost all evidence is now found in digital form.

Computer forensic experts should have strong academic backgrounds as well as practical experience in the very technical field of computer science. Knowledge and experience in security will also be essential in cases involving security incidents. The experts will also need to have specialized training and experience in the proper methodology required for computer forensic investigations.

Experts in computer forensics will be able to recover evidence that appears to have been deleted. Experts will also be able to retrieve evidence about a user's actions which is stored by computers, without the direct knowledge of the user. Additionally, experts will be able to draw conclusions based on the analysis of the digital evidence. Finally, experts will gather the evidence in a way that properly preserves its integrity so that it can be used in court if and when it is necessary.

# Enterprise Risk Management At A Glance

ERM professionals bring a unique mix of strong academic backgrounds complemented by professional experience ranging from "Big Four" consulting firms to major corporations and prestigious professional certifications. A snapshot of ERM's profile can be seen below:

## Education

### Qualifications

M. S. in Computer Information Systems  
M. S. in Information Networking  
M. S. in Management Information Systems  
Master of Accounting Information Systems  
Master of Business Administration

### Universities

Carnegie Mellon University, Pittsburgh, Pennsylvania  
Syracuse University, Syracuse, New York  
Xavier University, Cincinnati, Ohio  
University of Miami, Miami, Florida  
Florida International University, Miami, Florida

## Certifications

Certified Public Accountant (CPA)  
Certified Information Systems Security Professional (CISSP)  
Certified Information Systems Auditor (CISA)  
Certified Information Systems Manager (CISM)  
Certified Information Technology Professional (CITP)  
GIAC Security Essentials Certification  
GIAC Systems and Network Auditor  
Microsoft Certified Professional

## Prior Work Experience

PriceWaterhouse Coopers  
CERT® Coordination Center  
SONY Electronics Latin America, Inc.  
RJR Nabisco  
Diageo plc  
Arthur Young  
Carnegie Mellon CyLab  
Evertec Inc.  
American Bankers Insurance Group  
Chesebrough Pond's  
Starboard Cruise Services, Inc.  
Demotte Consulting, Ltd.

## Some of our Clients...

ABN AMRO Private Banking  
Bacardi-Martini, Inc.  
CitiBank  
Carnival Cruise Lines  
Commerce Bank  
Florida Power & Light Company  
Knight Ridder  
North Broward Hospital District  
Ocean Bank  
Rinker Materials  
Sylvania Lighting International  
The International Bank of Miami

**enterprise risk management**

*The Control Professionals*

299 Alhambra Circle, Suite 220,  
Coral Gables, FL 33134.  
P: (305) 447 6750 F: (305) 447 6752  
Email: [info@emrisk.com](mailto:info@emrisk.com) Web: [www.emrisk.com](http://www.emrisk.com)