Computer Forensics in a LAN Environment

Michael J. Corby, CCP, CISSP
M Corby & Associates, Inc.

Audience: Security Knowledgeable with varying backgrounds

The industry has, at long last, accepted Computer Security as a key component of any organization’s operating and strategic plan. There can be no doubt that preventing unwanted access to systems, files and the computer environment is a good thing. Furthermore, the accurate and data storage, retrieval and processing is crucial for success. But what happens if somewhere, somehow a chink in the armor is revealed. Do you have the procedures in place to identify that an “event” has occurred, how you can prevent future occurrences and how the situation was caused. Tracking the source of the problem and in some cases, establishing corrective measures and providing reliable and usable evidence for legal proceedings (if necessary) can pose a new challenge. Computer forensics is a new specialty that can identify the proper procedures for collecting evidence in a manner suitable for use in apprehending and prosecuting security violators.

The first part of this session will identify some of key elements in building an effective Computer Forensics program within the Computer Security practice area. Many areas will be covered including procedures, career issues, legal processes and financial justification.

The second part will focus on specific ways to configure clients and servers in a LAN environment to facilitate forensic data collection and establish proper evidence collection procedures. Platforms covered will include: Novell and Windows/NT servers; DOS, Windows 3.x, 95, 98 and NT clients. Attendees will review a checklist of parameters to specify and methods to use that maximize data collection and preservation.

Speaker Biography

Mr. Corby is CEO and Consulting Director for M Corby & Associates, Inc. a US Consultancy founded in 1989. He has been an IT Professional for over 30 years specializing in systems technology management and computer security. As a Technology Specialist, Systems Manager and CIO for large international corporations, and as Consulting Director of hundreds of Systems and Technology projects for several diverse companies, he has put many theories and creative ideas into practice. Prior to his term as the Consulting Director for M Corby & Associates, Inc., he was practice director for the IT Consulting Practice of Ernst & Young, CIO for a division of Ashland Oil and the Bain & Company Consulting Group. He is a Certified Information Systems Security Professional (CISSP) and Certified Computer Professional (CCP). In 1994, the Computer Security Institute awarded Mike the *Lifetime Achievement Award.*

Speaker Contact Info:

Michael J. Corby, CCP, CISSP
255 Park Avenue
Worcester, MA 01609
Phone (508) 792-4320
Fax: (508) 792-4327

E-Mail: mcorby@mcorby.com

Introduction to Computer Forensics

Michael J. Corby, CISSP

M Corby & Associates, Inc. USA

Abstract

- The industry, at long last, accepted Computer Security as a key component of any organization’s operating and strategic plan. There can be no doubt that preventing unwanted access to systems, files and the computer environment is a good thing. Furthermore, accurate data storage, retrieval and processing is crucial for success. But, what happens if somewhere, somehow, a chink in the armor is revealed. Do you have the procedures in place to identify that an “event” has occurred, determine how you can prevent future occurrences and how the situation was caused? Tracking the source of the problem and in some cases, establishing corrective measures and providing reliable and usable evidence for legal proceedings (if necessary), can pose a new challenge to the security professional. Computer forensics is a new specialty that can identify the proper procedures for collecting evidence in a manner suitable for use in apprehending and prosecuting security violators.
- This session will identify some of the key elements in building an effective Computer Forensics program within the Computer Security practice area. Many areas will be covered, including procedures, career issues, legal processes and financial jurisdiction.

About the Speaker:

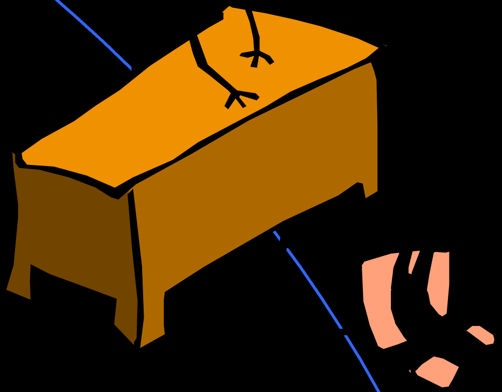
- Mr. Corby is Consulting Director for M Corby & Associates, Inc., an Information Technology Consulting organization founded in 1989. He has over 30 years of experience in Systems Operations, Technology Management, Application Design and Strategic Planning. His organization specialized in Computer Security, Effective IS Management and developing crisp, responsive IS Strategies. He has managed numerous projects including several with over 100 participants that lasted for up to four years. Previously CIO for Bain & Company and the Riley Stoker division of Ashland Oil, he also was Director of Technology consulting for Ernst & Young (formerly Arthur Young & Co.), and held management and technical positions with Thom McAn shoes and State Mutual (Allmerica) insurance. He is a Certified Computer Professional and Certified Information Systems Security Professional. Mike was the first-ever recipient of the CSI lifetime achievement award, and has spoken at conferences throughout the US, Canada, Mexico and Great Britain.

Objectives

- After this workshop, you should:
  - understand where computer forensics can be applied
  - understand the scope and relevance of computer forensics
  - learn some techniques for computer forensics
  - build a strategy for incorporating computer forensics into your computer security practice

Agenda

- Introduction
- Event identification
- Prevention/Mitigation
- Elements of Forensics
- Financial Implications
- Career Issues
- Platform Specifics
- Summary - Q/A



Introduction

- **What is computer forensics anyway?**

The application of computer investigations and analysis techniques in the interests of determining potential legal evidence. Computer specialists can draw on an array of methods for discovering deleted, encrypted, or damaged file information (Robbins, 1997).

Event Identification

- Human Behavior
  - blackmail
  - extortion
  - disgruntled employee
  - obtuse behavior
  - “dropping the dime”
  - sabotage/corporate espionage

Event Identification (2)

- Physical Behavior
  - flood, fire, earthquake, etc.
  - mechanical failures
  - physical access prohibited
  - theft/damage

Event Identification (3)

- Organizational Issues
  - operating system upgrade
  - new hardware
  - new software

Event Identification (4)

- Operational Issues
  - disk failure
  - backup
  - virus
  - accidental deletions (oops!)
  - overwrite

Prevention/Mitigation

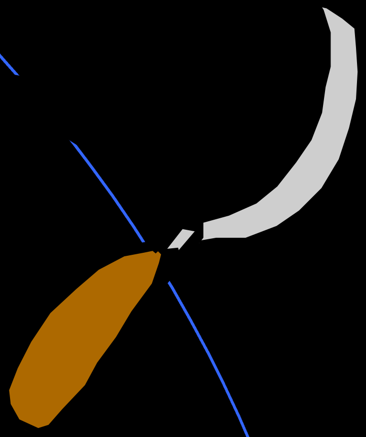
- Procedural
- Disaster recovery plan
- planning by project manager
- purchasing hardware & software (data security)

Indirect Results of these Events

- Loss of service
- Discontinuity of reporting
- Profit loss

Elements of Forensics

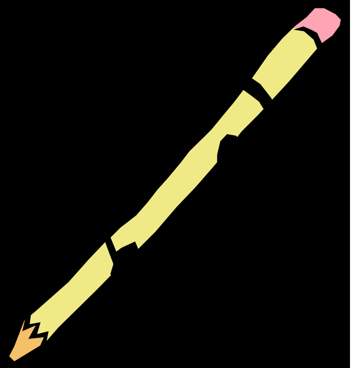
- Recovery
  - evidence preservation
  - damage control
  - system restoration
- Causation (problem source)
- Proof
  - evidence analysis



Objectives of Forensics

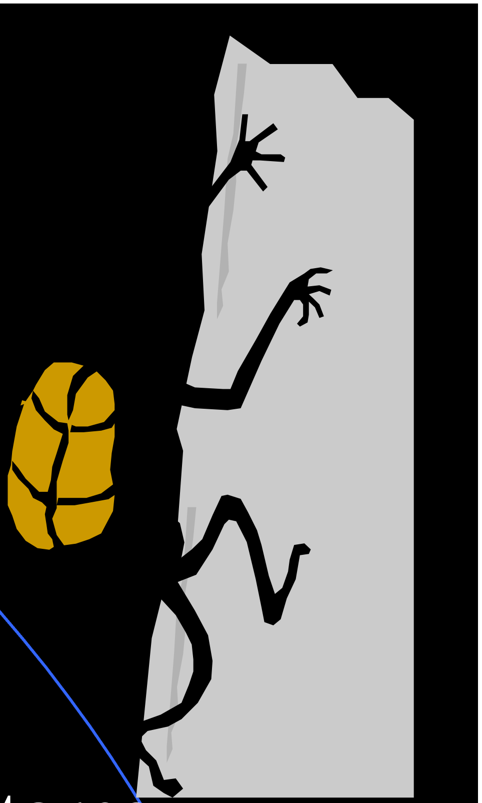
- Prove it in court (legal)
- Prove it to prevent future incidents (business)

Financial Implications



- Insurance for theft/loss
- E & O (???)
- Purchase of extra hardware for incident potential and response
- Risk to business
- Cost of prosecution
- Loss/new business (e.g., no controls = loss of clientele and sound controls = increase in clientele)

Career Issues



- Types of careers
  - forensic consultant
  - legal aid
  - computer crime expert/investigator/attorney
  - government agent (High Tech Unit, AG, FBI)

Career Issues (2)

- Drawbacks
  - education
  - unknown factor (industry lacking knowledge about this area)
  - no uniform standards to establish expert status
    - experts necessary for court cases to offer opinions
    - must have ability to explain process in NON-TECHNICAL MANNER
  - TIME AND LABOR INTENSIVE!!!

Q & A

Summary

- Computer Forensics is an important element of any Security Program.
- Problem recovery may be quicker if reactive, but may not yield stability.
- Weigh the importance of 3 factors:
  - Restoration
  - Prevention
  - Prosecution
- As with anything else: Stay Current!

Platform Architecture I

Windows NT

Platform Architecture II

Windows 95/98

Platform Architecture III

DOS/Windows 3.1x

Comments and Observations

Bibliography of References

- Burton, R.F. (1996). “Searching for Fraud Behind the Screens,” *The White Paper*, Vol.. 10 (2), The Association for Certified Fraud Examiners
- Forgione, D. (1994). “Recovering “Lost” Evidence from a Microcomputer,” *The White Paper*, Vol.. 8(3), The Association for Certified Fraud Examiners
- Clede, Bill (1993). Investigating Computer Crime is Every Department’s Concern, *Law and Order*, July 1993. Available for FTP at: `ourworld.compuserve.com/homepages/billc/compcrim.htm`
- Conly, C.H. & McEwen, J.T. (1990). Computer Crime: The New Crime Scene. NIJ Reports No. 218, National Institute of Justice, Office of Justice Programs, U.S. Department of Justice
- Farwell, W. L. (1997). “Stand-alone PC Examinations: Some Basic Forensic Guidelines,” High Technology Crime Investigation Association Newsletter, New England Chapter, Vole. 2(1).

Bibliography (2)

- **Howell, F.J., Spernow, W. and Farwell, W.L. (1998). “Computer Search & Seizure and Computer Forensics,” HTCIA Training Seminar in Boston, MA, April 1998.**
- **Robbins, J. (1998). An Explanation of Computer Forensics by Judd Robbins. Available at `knock-knock.com`**
- **Rosenblatt, K.S. (1995). *High Technology Crime: Investigating Cases Involving Computers.* San Jose: KSK Publications**

If You Would Like More:

Michael J. Corby, CCP, CISSP

M Corby & Associates, Inc.
255 Park Avenue, 8th Floor
Worcester, MA 01609-1946 U.S.A.
Phone: 1 (508) 792-4320
Fax: 1 (508) 792-4327
Web: www.mcorby.com
E-Mail: mcorby@mcorby.com or lpaul@mcorby.com