

## Developing Corporate Policies in Support of Computer Forensics

### Abstract

Computer Forensics has become a buzz in today's world of increased concern for security. It seems any product that can remotely be tied to network or computer security is quickly labeled as a "Forensics" application. This phenomenon makes architecting clear incident response plans and corporate security plans which support computer forensics difficult. Today's corporate climate of increased competition, cutbacks and layoffs makes it essential that corporate security policy and practices support the inevitability of future litigation.

This whitepaper is intended to raise awareness of what computer forensics is... is not, and identify crucial questions for corporate planning in support of computer forensics. Answering the questions raised in this whitepaper will assist managers in creating sound corporate security policies and practices that support computer forensics.

### Background

The first step in defining the need for computer forensics in the corporate environment is to understand just what we mean when we say "computer forensics". The word *Forensics* can be defined as "Pertaining to the law". With this definition in mind the term *Computer Forensics* can be defined as "computer science in support of the law".

As discussed, today's corporate climate mandates preparation for the possibilities of future litigation. Preparation for such possibilities from an IT (Information Technology) perspective requires managers ask two questions.

- What IT policies can I put in place to support the legal process?
- What can Computer Science and IT departments do to support the legal process?

By answering these questions, IT managers are well on the road to “Prior Planning Peace of Mind”. Issues managers should focus on to ensure security policies support the legal process include acceptable use policies, logon banners, and user responsibilities.

A good reference for creating security policies is “Information Security Policies Made Easy (Version #7)” by Cresson and Charles Wood published by Baseline Software; ASIN: 1881585069.

As for the second question let’s take the divide and conquer approach by categorizing some areas of interest:

- Network Design and Procedures
- Desktop Support Procedures
- Incident Response Procedures
- Employee Activation & Termination Procedures (IT)

One approach to answering the second question, *how to support computer forensics* in each of the areas of interest is to understand how computer evidence is challenged in court. Generally the opposing legal team will make challenges to evidence authenticity. That is to say “Were the forms, records or data altered?”, “Was the program that generated the forms or data reliable?”, “What is the true identity of the author?”, “Were times reliable?”, and sometimes the integrity of people involved.

The first area of interest, *Network Design and Procedures* contains several items which can help mitigate evidence challenges.

1. Ensuring accounting, authentication & auditing systems/procedures are in place which identify and log user actions within the network. General use or group accounts and allowing users to disclose passwords to others nullify efforts of authentication and auditing.
2. Time Servers and standard time settings are essential to ensuring audit trails are discernable.

The second area of interest, *Desktop Support Procedures* contains items many organizations overlook.

1. As employees come and go within organizations they are often assigned computers recently assigned to and used by others. This procedure can make it difficult to tie data and audit trails found to a specific person. A procedure which helps eliminate challenges that data or audit trails found on a system did not belong to the user assigned is to create a fresh operating system image to a forensically clean disk when issuing any computer to a new user. By a *forensically clean* disk we mean a drive that has been wiped (erased) to clearing and sanitizing standard DOD 5220.22-M or at least a new shrink-wrapped drive.
2. Utilizing a standard set of desktop applications which are known to perform to expectations can help alleviate attacks against application behavior.

3. Additionally it is recommended not to allow user installed applications without testing and approval by IT professionals.

The third area of interest, *Incident Response Procedures* contains items which are routinely the focal point for computer forensics.

1. Many incident response plans contain references to computer forensics, yet fail to fully address the issue. Ensure incident response plans contain well documented, sound methodologies for incident response teams which support the four phases of computer forensics (Identification, Collection/Preservation, Analysis, and Reporting).
2. Some organizations do not have the resources to fully train first responders in computer forensics. For such organizations it is essential that at a minimum “Bag & Tag” as well as physical chain of custody procedures be implemented.

Best Practices in these areas can be found in “Electronic Crime Scene Investigation – a guide for first responders” (<http://www.ncjrs.org/pdffiles1/nij/187736.pdf>) and at the International Association of Computer Forensics Specialist web site at <http://www.iacis.com/>

*Employee Activation / Termination Procedures* is the area where a few steps can make the difference.

*Scenario:* A common situation is one in which Employee A leaves Company B to work for Company C. Shortly thereafter Company C shocks the industry by announcing a product which is very close to the super-secret product Company B was working on. When Company B starts an investigation they find that the notebook computer Employee A had returned when leaving the company was already issued to another user. A human resources manager from Company B then ask a system administrator to retrieve and review Employee A’s old notebook computer. Not being trained in computer forensics the system administrator makes several serious procedural mistakes when reviewing Employee A’s old notebook computer. Despite recovering some evidence which had been deleted on the computer, no evidence was useful since no less than three people (two employees and a system administrator) had made significant changes to the computer and therefore any evidence.

1. To prevent the scenario above, as well as support future unknown HR actions, many companies are creating forensic images of workstations and notebook computers upon the employee’s termination no matter what the characterization of the termination. This approach can require a large amount of dedicated data storage space highlighting the need for a balanced approach. Some organizations are choosing to select an executive or director level cut off for such a procedure while others are lowering the bar to all managers and above. No matter the approach, it is easy to justify some added IT expense with the possibilities of defending a multi-million dollar law suit, or recovering crucial evidence needed to prosecute in the above scenario.
2. Some companies are taking the procedures above one step further by performing rudimentary forensic analysis of the image once taken to provide early warning of possible employee misconduct. Organizations taking this approach should ensure

extensive training and qualifications are provided for the persons conducting the forensics analysis.

Note a forensics image is bit-stream image of the original drive including all available file slack space and unallocated sectors of the disk. The National Institute of Standards and Technology Disk Imaging Tool Specification available at <http://www.cftt.nist.gov/> describes recommended performance requirements for tools that create bit-stream images used in computer forensics.

While some may believe implementing all the measures mentioned would be overkill, this paper is intended to raise questions and awareness. Each organizations needs are unique and may contain additional areas of interest, designs and procedures that can support computer forensics. Following the suggestions outlined will put most companies well on the road to a successful support program.

### **Conclusion**

The need for corporate focus on computer security and forensics is clear. Any company which has experienced litigation without taking any of the measures discussed should easily be able to make a business case based on ROI alone for supporting computer forensics preemptively. Implementing support for the computer forensics process during planning and design can be essential for a company's successful success in, or prevention of litigation.