Proceedings of the 9th Colloquium for Information Systems Security Education
Georgia Institute of Technology
Atlanta, Georgia, 6-9, June 2005

Corporate Computer Forensics: Opening Opportunities for Students

Patricia Y. Logan, Ph.D.

Abstract--In addition to managing the security of data assets, Information Technology (IT) has taken a significant role in managing the enforcement of corporate Acceptable Use Policies (AUPs). Human Resource departments rely on IT to monitor employee adherence to these policies. The ability of IT to monitor and investigate suspicious employee behavior and the direct violation of corporate AUPs represents an important element of managing information security. IT staff use some of the same computer forensic skills practiced by law enforcement, but investigations often require an extension of those skills to meet the unique nature of corporate surveillance and investigation. The majority of courses in computer forensics focus on the skills sets required for law enforcement yet the majority of information systems (IS), computer science (CS), and information security students accept positions in a corporate setting. These students would benefit from a course that focused on computer forensic skills applied to corporate investigations. The author proposes a course in corporate forensics and investigations that can serve as an elective for both IS/CS and security majors.

I. INTRODUCTION

In the triad of people, policies, and technology that represent security enforcement in the corporate setting, the Acceptable Use Policy (AUP) represents the set of allowable actions that employees may perform with respect to computer and network use. The scope of AUPs includes most of the IT responsibility landscape: Internet usage, email, the use of computer hardware and software, and network services. Corporations increasingly rely upon Information Technology (IT) staff to monitor and investigate employee misbehavior in using computer and network resources.

The majority of major U.S. corporations monitor their employees by checking their e-mail, Internet, phone calls, computer files, or by videotaping them at work. The need for monitoring and investigation is driven by concerns for improving employee productivity, increasing security, reducing employee misbehavior, and protecting the investment in network bandwidth. An American Management Association study of private-sector companies from 1997-2000 revealed that sixty-three percent of the companies surveyed monitor their workers' internet connections and forty-seven percent store and review employee e-mail.. According to a survey by International Data Corp (IDC): 30% to 40% of internet access is spent on non-work related browsing (International Data Corp., 2000); 60% of all online purchases are made during working hours; 41% admit to personal surfing at work for more than three hours per week. Managers are especially aggravated by complaints that Internet surfing uses up a large portion of the work day and is borne out by estimates of 30% - 40% of lost productivity accounted for by cyber-slacking [1].

The loss of productivity is a significant worry for corporations but the loss of profits from criminal acts and the ensuing bad publicity is a larger fear. Approximately 80% of computer crime in the finance industry is committed by "insiders" (http://www.intrusic.com/Experts.htm). Recent evidence supports the reality that the majority of unauthorized intrusions are performed by existing employees, consultants or others with a relationship to the company and computer access [2]. The FBI's CCIPs (Computer Crime and Intellectual Property Section) web site documents that over 50% of the intrusions investigated and referred for federal prosecution involved intruders with a relationship to the company they attacked (e.g., U.S. v Blum, U.S. v Eitelberg, U.S. v Sandusky, U.S. v Lloyd) [3]. Insiders managed to steal $100 million by some estimates; $1 billion by others. The average fraud inflicts a loss of about $110,000 per corporate/organization victim. Approximately

Marshall University Graduate College
College of Information Technology and Engineering
South Charleston, West Virginia

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

60% of security breaches occur within a company - behind the firewall. Of Fortune 500 organizations, 27% have defended themselves against claims of sexual harassment stemming from inappropriate email (including Chevron and Microsoft that settled sexual harassment suits based on circulated emails for $2.7 million a piece) [4]. Given this evidence of potential harm in is easy to understand why corporations have undertaken employee surveillance as a means of loss prevention.

In the last few years there have been a number of high-profile companies that have used violations of their corporate AUPs to discipline employees. For example, Xerox Corporation terminated 40 workers for surfing pornography and shopping web sites; Dow Chemical terminated 50 workers and disciplined 200 for emailing pornographic and violent images from company computers (www.fcw.com/civic/articles/2000/oct/civ-shadow-10-00.asp); the NY Times, Edward Jones, and First Union Bank all terminated employees for sexually explicit email messages. Surveys have shown that 60% of corporations have disciplined employees and 30% have terminated staff based on AUP enforcement by IT [5]. AUPs provide both the permission to monitor (through employee agreement) and the list of unacceptable practices that IT will be asked to monitor. For Human Resources, employee monitoring is the perfect compromise for providing unlimited network access.

Table 1

Surveillance Activity	**1997**	**1998**	**1999**	**2000**	**2001**
Storing and reviewing computer files	13.7	19.6	21.4	30.8	36.1
Storing and reviewing e-mail	14.9	20.2	27.0	38.1	46.5
Monitoring Internet connections	NA[1]	NA[1]	NA[1]	54.1	62.8
Clocking overall computer use	16.1	15.9	15.2	19.4	18.9

[1] Not available
[6]

Table 1 demonstrates the trend in managing employees by surveillance and investigation through the direct action of IT. The table reveals an increasing percentage of corporations asking their IT departments to enforce AUPs. In the author's experience as a senior manager in the banking and insurance industries, these numbers are lower than would be seen in more regulated corporations. As IT departments hold the expertise in managing the infrastructure, they become the logical choice for managing the access and use of these corporate assets.

II. HOW PREPARED IS AN IT DEPARTMENT TO ASSUME THE ROLE OF ENFORCER?

IT staff can be involved in investigations for civil litigation, as well as investigations that include a wide range of potential crimes: breaches of confidentiality, deliberate corruption of data, fraud, vandalism, child pornography, theft, hate speech, identity theft, copyright violation, extortion, industrial espionage, systems sabotage. Insurance companies and financial institutions may have separate investigative units to mitigate costs by using discovered computer evidence of possible fraud in accident, arson, workman's compensation, theft, and embezzlement cases. Additionally, IT departments will maintain a CIRT (Corporate Incident Response Team) for investigations of more widespread incidents. Corporations realize that maintaining a knowledgeable internal IT staff is the most cost effective means to provide these services [7].

In the corporate setting IT departments will need to have knowledgeable staff in computer forensic investigations. IT staff in the corporate environment use many of the same computer forensics methods of investigation as law enforcement. Monitoring, surveillance, and investigation are generally not the responsibility of a corporate CIRT because many of the cases may not be true incidents in the classic "intrusion" sense. In order to perform these activities IT staff need to extend the basic computer forensic skills to include the following:

- Evaluation and installation of email and web filters
- Manage and monitor access to resources and data

ISBN 1-933510-99-4/05/$15.00

- Scan emails for inappropriate content
- Scan storage for inappropriate or suspicious files
- Perform back-ups on network shares and desktops/laptops for forcibly terminated or senior level employees
- Monitor network use
- Interpret output from monitoring tools
- Investigate virus and worm infection vectors
- Provide electronic evidence pursuant to a subpoena or warrant

Clearly, the sum of these activities will extend the knowledge required beyond the basic skills of computer forensics practiced by law enforcement. Are there different skills required of corporate investigators versus law enforcement? The answer to the question is in the affirmative as there are differences in focus, frequency, law, investigation outcomes, skills, tools, and perpetrators that make the practice of corporate computer forensics unique.

A. Differences in IT and law enforcement practice of computer forensics

There are a number of points of divergence in the practice of computer forensics in the corporate setting. The major differences are summarized into the areas of investigative focus, frequency of surveillance and investigation activity; laws governing private investigations, the outcome from an investigation, the IT skills required for corporate investigators, the tools used by corporate investigators, and the perpetrator of the violations or crimes.

Focus: Corporate investigations must not compromise business operations

In the corporate setting, monitoring an employee's behavior and performing an investigation happens concurrent with normal business operations. Interference with business operations can result in a loss of productivity, discovery by investors and the press resulting in negative publicity, and can impact the operations of a variety of business activities such as customer support, sales, and management. IT is positioned to act as a service organization and understands this corporate environment.

Frequency: Employee monitoring may be routine

In the corporate setting, everyone is under surveillance. IT will be required to interpret AUP violations or crimes from a large volume of data contained in logs and reports from a variety of tools and then correlate them to a specific employee. In the course of monitoring for compliance with AUPs and in conducting normal infrastructure management functions, IT staff will "discover" evidence of violations or crimes.

Law: Perpetrators have provided permission for monitoring

Best practices in information security include the requirement that AUPs be developed in conjunction with corporate counsel and signed by employees acknowledging that the corporation "owns" the hardware, software, and networks and can, therefore, monitor, search, seize, discipline, and terminate employees for violations of internal policy or law. The usual constraints on "search and seizure" required for government agents (i.e., law enforcement) generally do not apply in the corporate environment.

Outcomes: Investigations may result in internal disciplinary actions rather than criminal prosecution

IT departments work at the request of human resources and company management in consultation with corporate legal counsel. The evidence gathered in the course of monitoring or investigation will be used to substantiate a disciplinary action and possibly defend against a wrongful termination suit if the discipline includes a forcible termination. Corporations seldom prosecute employees, as it exposes them to public attention and a potential loss of profit and stock value.

Skills: IT controls the corporate technologies

IT departments determine the computing and networking needs of the corporate environment and define the desktop/laptop images, software, and network access. IT easily recognizes differences from their image and additions of unapproved software or hardware in excess of that originally installed. The creation of images and network access constraints can be designed

ISBN 1-933510-99-4/05/$15.00

to facilitate monitoring, prevention, and investigation.

Tools: IT will not use the same tools to monitor or investigate

IT departments are seldom in a position to support a large budget for a dedicated forensic tool such as EnCase. Usually, the tool sets are lower in cost and require knowledge of more than a single tool. Additionally, the tool sets include a broader range of function from monitoring to investigation across a diverse hardware and software landscape that includes multiple versions of operating systems and software.

Perpetrators: Insiders are the focus of most monitoring, surveillance and investigation

The perpetrators in a corporate environment are insiders with access to data assets, knowledge of the monitoring tools, an understanding of AUP violations, authority to use corporate resources and potentially individuals with substantial responsibility for corporate profit.

The cost of out-sourcing surveillance and investigation is often prohibitive and IT departments resort to sending their staff to courses provided by vendors such as Foundstone, NTI, or Guidance in order to use computer forensic tools. Many traditional courses of study at the undergraduate and graduate level have not offered content that meets the needs of corporate investigators. While many universities are now offering computer forensics, the courses mostly focus on the needs of first responders in law enforcement. Perhaps it is time to suggest a new course that focuses on the differences in the practice of computer forensics in the corporate setting?

III. A NEW COURSE PROPOSAL

Why suggest a separate course? Computer forensics is practiced in two primary settings: law enforcement and corporate practice, but courses in computer forensics usually teach from the perspective of law enforcement. Computer forensics textbooks and even practice guidelines (including the only definitive guide to search and seizure authored by the FBI) are mostly focused on criminal investigations where evidence can be conveniently searched and examined in a lab without considerations involving a continuance of business operations. IT staff are often pressed into service without a clear understanding of the legal requirements, an absence of documented procedures, validated tools, and technical capabilities. Sloppy investigations can lose evidence for prosecution, corrupt or spoil evidence, or subject the corporation to wrongful termination lawsuits.

How would IS/CS graduates employed as members of an IT Department for a large corporation deal with the following scenario?

Employee Sam Smith checks into the office at 9:35 a.m,. but does not use his key card this morning because Sally held the door for him. John then logs onto the NT/Novell servers at 10:00 a.m. and prints 97 pages on a department color printer. Sam then makes 50 copies on the copy machine, spends 160 minutes on his desk phone, while at the same time visiting a pornography and auction web site, transfers 123 Mbytes of JPEG images to a friend at another company, uses some unknown protocol to communicate with various devices on the Internet, infects his workstation with a virus hidden in a 2 gigabyte download at 3:23 p.m., logs into a server on the corporate network to access a password-protected file which he copies to a thumb drive, and goes home at 4:00 p.m. At 4:30 p.m., Sam's inactivity timer locks his workstation screen. Meanwhile, Sam's PC begins to infect surrounding systems with his newly acquired virus, and from home he transfers the copied file to a remote address in Asia using the corporate VPN [6].

This scenario conveys the complexity of a corporate investigation and the variety of monitoring tools that are required, as well as the variety of simultaneous activities that can happen in the corporate setting. A traditional course of study in IS/CS may not provide an adequate investigative skill set or preparation for the complexity of the corporate IT setting.

The author surveyed a number of computer forensics courses listed on the Internet by universities and colleges where a syllabus or detailed course description was available (about one-third were behind WebCT or Blackboard Portals) and found that the majority of courses

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

did not include many of the activities of a corporate investigator; assumed the use of EnCase as the primary investigative tool; ignored the monitoring and investigation of insider activities; and did not provide guidance in enforcing AUPs.

Textbooks in computer forensics also assume law enforcement careers, that corporate investigations always use an incident response format, the primary perpetrators are criminals/hackers external to the corporation, and over-emphasize the investigation of network activities. While the focus for employment in computer forensics remains law enforcement (federal, state, local), what happens to the majority of our IS/CS graduates who go into the corporate environment and will be assigned to the role of corporate investigator? Should students not declaring an information security major or emphasis be provided a course to support their future corporate activities? Would students intent on a career in government need the corporate skills for a later career move into corporate investigator?

A separate course in corporate forensics can be used in conjunction with an information security track or as a separate elective within IS/CS programs of study. This course would provide the necessary skills to enable the future corporate IT professional to conduct effective investigations and provide an IT department with direction in the best practices for corporate investigations. Ideally, the course should include the use and selection of tools such as password crackers, data recovery, shredders, encryption, tool sets used by employees for data hiding, and imaging. The skills to read and interpret a variety of system, IDS, firewall, and network surveillance logs must also be included. Investigation methods that consider disaster recovery and business continuity are also needed. Student exercises should include using tools, selecting and validating tool sets, setting up surveillance to enforce AUPs, and mock exercises in retrieving data, evaluating evidence from multiple sources, and writing a report.

Pre-requisites for the course should be the ability to use, install, and configure Windows, UNIX systems, and the Mac (a favorite in marketing and public relations departments), as well as basic network skills. Specific topics and exercises are proposed in Table 2.

Course objectives and skills should revolve around a student's future role in a corporate setting. The author has included these topics in undergraduate and graduate courses in forensics. Students have enjoyed exercises that involved: setting up a monitoring environment to enforce AUPs; converting classroom space into a simulated office for investigation; and setting up a variety of crime scenes within the corporate setting using desktops, laptops, and storage media for students to "solve". Asking students to create their own crime scene for other teams to solve as a capstone exercise has provided the author's students with an appreciation of the complexity and inter-relatedness of evidence in the corporate setting.

For those schools with a limited budget to offer a formal computer forensics program (that normally requires expensive software and hardware) a course in corporate forensics can cost much less. Many of the software tools are available for a reasonable cost. Students can download many tools as demonstration versions. A classroom set-up for the course can make use of discarded campus desktops and laptops (including Macs) that can be imaged in a variety of OSs for student exercises.

Would students that have taken a traditional law enforcement-focused course in computer forensics be unable to succeed in the role of corporate investigator? Some of the skills would directly translate to the corporate environment but they would still need the additional knowledge outlined in this course proposal to completely succeed. A student that has taken both a traditional computer forensics and a corporate forensics course would possess a complete skill set and be a desirable "property" in the job market.

IV. CONCLUSION

CS and IS programs can boost student interest in their major by providing a separate course in corporate forensics. Information security students will have a more robust background taking both a law enforcement focused course and one that involves the unique corporate aspects. The coursework will strengthen their

ISBN 1-933510-99-4/05/$15.00

resume for employment in the corporate world, and will be more appealing to corporate employers because of these unique skills.

V. REFERENCES

[1] http://www.snapshotspy.com/employee-computer-abuse-statistics.htm

[2]www.gocsi.com/db_area/pdfs/fbi/FBI2003.pdf

[3] www.ccips.gov

[4]http://www.dmreview.com/article_sub.cfm?articleId=3285

[5]http://www.cerberian.com/02products_abusestats.htm

[6]www.techreview.com/articles/03/04/farmer0403

[7]http://www.cio.com/archive/060102/et_article.html

Table 2.

Knowledge	Exercise
Creating a validated forensic tool kit	Students investigate, validate and assemble a set of tools
Finding evidence on a drive or other media	Students will be provided with a disk with evidence of one or more AUP violations or crimes
Patterns of file naming and organization (indicator of CP)	Students will be provided with a disk with simulated evidence of child pornography
Restoring/recovery of disks and data	Students will receive a disk with data that has been erased and recover the data for analysis
Erasing data	Students will use and evaluate tools for erasing data
Registry examinations	Students will review a registry for evidence of new software installations and presence of spyware or malware
Areas for data hiding (swap, temp, hidden files)	Students will find hidden evidence on a disk located in the swap, temp or other hidden areas
Identifying encryption and steganography	Students will use DOS, Quickview, NTI tools to identify encrypted data
Image a hard disk	Students will use a variety of tools including Norton Ghost to image media
Tools used by end-users to prevent detection	Students will identify tools available to hide evidence on a desktop
Recovering data from PDAs	Students will recover data from a PDA and identify files on the desktop that may represent PDA back-up data
Using remote control tools (Symantec's pcAnywhere; Citrix's ICA Client, used with MetaFrame on a server; or Microsoft's SMS Client to monitor employees	Students will use and configure a remote control tool to monitor a session
Investigating network "choke points" (authentication servers, authorization servers, directory servers, database servers, file and print servers, access routers, firewalls, proxy servers, mail servers, and VPN gateways) for download abuse	Students will review a variety of syslogs for evidence that an employee is mis-using network resources
Ability to review cookies, running processes, recycle bin, MS Office for revisions, backups and auto-complete	Students will identify places where evidence can be correlated to prove a violation or crime Students will identify best practices in client images that facilitate security investigations
Password recovery and restoration of access (Knopix, BartPE)	1) Students will use password cracking tools to recover document passwords; 2) Students will use network access tools to gain access to network resources from a client machine
Install and configure keyloggers	Students will use and configure a keylogger to gather and interpret evidence
Identifying and documenting evidence from logs	Students will use a variety of intrusion detection products and examine log output for evidence of violations or crimes
Detecting use of media	Students will be able to identify external media devices used on a client machine
Identify timelines	Students will use a variety of evidence to construct a timeline for a violation or crime
Developing a methodology	Students will have a final exercise that requires substantiation of an investigative methodology
Thinking like an investigator	Students will have a capstone exercise that requires them to identify a violation or crime

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE