Cyber crimes, intrusion detection, and computer forensics

Michael S Luehlfing, Cynthia M Daily; Thomas J Phillips Jr; L Murphy Smith
Internal Auditing; Sep/Oct 2003; 18, 5; ABI/INFORM Global
pg. 9

Cyber Crimes, Intrusion Detection, and Computer Forensics

Electronic crimes are often mirror images of their paper-based counterparts, and can cost companies dearly.

B
illions of dollars are lost each year due to "cyber crimes," also referred to as computer crimes, electronic crimes, or e-crimes. "Cyber" is short for cyberspace, the electronic medium of computer networks, in which online communication takes place. There are numerous news stories regarding electronic crimes and the related costs to companies. Though control techniques and other security policies and procedures are critical to the deterrence of electronic crimes, detection and resolution of successful or attempted electronic crimes are also of critical importance. Not only the cost, but also the embarrassment of such crimes is something that all companies wish to avoid. This article focuses on electronic crimes, intrusion detection, and computer forensics. Armed with information on these topics, internal auditors can enhance their firms' abilities to detect and resolve electronic crimes.

A good example of an e-crime concern. Egghead.com, Jeff Sheahan, the president of Egghead.com, Inc., sent an e-mail to thousands of customers and their credit card issuers, notifying them of an attack on the company's computer system. After several weeks of investigation by the FBI and a forensic security firm (hired by Egghead.com), Egghead.com announced that its existing security system apparently interrupted the intrusion in progress. Although initial evidence indicated that approximately 7,500 credit card accounts in the system might have been affected, evidence gathered by the forensic team showed that no credit card numbers were obtained from the site. Not only Egghead.com, but all e-commerce companies will pay the price for high-profile security violations, in the form of reduced sales. Quick resolution of such intrusions is vital to a company's well being.

Common electronic crimes

Exhibit 1 highlights several common crimes, including their paper-based names as well as their electronic counterparts. In most cases, it is the same old crime, just electronic rather than paper-based. In essence, the paper-based name is

MICHAEL S. LUEHLFING, Ph.D., CPA, CMA, is an associate professor in the School of Professional Accountancy at Louisiana Tech University.
CYNTHIA M. DAILY, DBA, CPA, is an assistant professor of accounting at Winthrop University in Rock Hill, South Carolina.
THOMAS J. PHILLIPS, JR., Ph.D., CPA, is the director of, and a KPMG endowed professor in, the School of Professional Accountancy at Louisiana Tech University.
L. MURPHY SMITH, DBA, CPA, is a professor in the Accounting Department at Texas A&M University.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
### EXHIBIT 1: From Paper-Based Crime to Cyber Crime

<table>
<thead>
<tr>
<th>Crime</th>
<th>Paper-Based</th>
<th>Electronic Counterpart</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forgery</td>
<td>Photocopy</td>
<td>E-mail spoofing</td>
</tr>
<tr>
<td>Data manipulation</td>
<td>False</td>
<td>Data stealing</td>
</tr>
<tr>
<td>Unauthorized access</td>
<td>Breaking</td>
<td>Password theft</td>
</tr>
<tr>
<td>Theft of intellectual assets</td>
<td>Dumpster diving</td>
<td>Software piracy</td>
</tr>
<tr>
<td>Damage</td>
<td>Arson</td>
<td>Virus/denial of service</td>
</tr>
</tbody>
</table>

changed to reflect the cyber nature of the electronic scheme.

**E-mail spoofing** (also known as **IP spoofing**) refers to electronic crimes in which a fictitious document (e.g., a message) is sent from a perpetrator disguised as a trusted colleague, customer, or vendor. The danger here is that members of the victim organization may make inappropriate decisions based on the information contained in the fictitious document. In essence, this electronic crime is similar to counterfeiting or falsifying a purchase order (or other document) using a copying machine.

Whereas e-mail spoofing relates to misleading electronic correspondence, **data d Hick** involves false electronic data. Whether paper-based or electronic-based, false inputs lead to false outputs. Accordingly, data d Hick ultimately leads to inaccurate reporting and, in turn, inappropriate and often embarrassing decisions.

**Password sniffing** is the automated guessing of user IDs, passwords, or phone numbers. In essence, the electronic criminal uses this information to “break and enter” into a system. Sniffing devices are often installed on the premises of victim organizations by electronic criminals disguised as employees, contract service providers, or even janitors. Once the system is penetrated, the electronic criminal may attempt to gain access to certain sensitive information, interrupt access to computer resources (i.e., deny service) or just leave some “clever” graffiti. A similar approach is **piggybacking**, which is a process of following a legitimate user through security.

Corporate spies have long been known to sift through garbage in search of trade secrets or other sensitive information. By hacking propriety software or databases instead of diving into garbage containers, the electronic criminal can increase his or her effectiveness and smell like a rose. In essence, this electronic crime is a form of software piracy.

**Denial of service** is an electronic crime where the intention of the perpetrator is to incapacitate, or dramatically reduce the availability of an organization’s computer resources. This would include bombarding websites with fictitious transactions or spurious inquiries. Like arson, viruses and worms can cause serious damage—temporarily at best, permanently at worst.

Although insiders, such as disgruntled or dishonest employees, are the most likely perpetrators of electronic crimes, the balance is shifting toward outsiders such as unscrupulous competitors or thrill-seeking hackers. Exhibit 2 provides statistics for detected cyber crimes during four recent years—1997 through 2000. A growing concern is that an increase in the quality of hacking tools coupled with the fact that only a small percentage of attacks are detected has created a feeling of safety for system intruders.

Numerous preventive measures, such as passwords, firewalls, encryption, and other security policies and procedures, exist to deter electronic criminals. However, given that such preventive measures are not always successful, electronic crime detection represents the last line of defense regarding loss prevention, or at least loss minimization.

### Electronic crime detection

Typically, electronic crimes are detected by one or more types of intrusion detection techniques. Such detection techniques include:

- tripwires;
- configuration checking tools;
- honey pots;
- anomaly detection systems; and
- operating system commands.

A brief overview of each of these intrusion detection techniques follows.

**Tripwires** are software programs that take snapshots of key system characteristics, which can be used to detect critical file changes. In this regard, tripwires provide evidence of electronic crimes because most intruding hackers make modifications when they install backdoor entry points or alter file system and directory characteristics unknowingly while snooping.

**Configuration checking tools**, also called **vulnerability assessment tools**, refer to software pro-
grams used to detect insecure systems. Though configuration checking tools are primarily preventive in nature, their use as monitoring devices can also provide evidence regarding electronic crimes. Specifically, configuration checking tools can be particularly useful in detecting suspicious patterns of system misconfiguration that might be malicious in nature. Admittedly, further investigation will be necessary to determine if a system misconfiguration is an electronic crime.

*Honey pots* (or *honey pot lures*) are employed to entrap and keep an electronic criminal occupied long enough to allow for identification and even apprehension of the perpetrator. These lures can be bogus system administration accounts, fictitious product or client information, or any myriad of created files that appear to contain sensitive information. In addition to facilitating perpetrator identification, honey pots also store evidence of the electronic crime itself.

*Anomaly detection systems* focus on unusual patterns of activity. In essence, anomaly detection systems develop and analyze user profiles, host and network activity, or system programs in hopes of discovering deviations from expected activity. Unusual keystroke intervals, abnormal commands, and unconventional program activities can provide evidence regarding the existence of an electronic crime.

Intrusion detection is also possible through the use of certain *operating system commands*. For example, checking log files and comparing outputs of similar programs are among the numerous manual techniques involving operating system commands. Typically, these commands are used on a daily basis by system administrators to search for evidence suggesting the possibility of electronic crimes.

In addition to manual procedures associated with the operating system commands, numerous other everyday procedures also provide evidence regarding electronic crimes. For example, checking empty log files (perhaps a symptom of someone trying to hide their activity), checking websites for information on the latest computer threats, and checking lists of known perpetrators and their hosts of origin are sometimes simple ways to provide evidence, as well as to discover ways to deal with new threats.

### Intrusion detection—additional considerations
For all of the positive aspects of the intrusion detection systems described above, there are a few caveats. First, intrusion detection techniques are fallible. For example, they might be disabled by an intruder or otherwise fail. Similarly, evidence derived from intrusion detection techniques may become tainted due to typical annoyances, such as data storage filling up or log files becoming corrupted. Accordingly, a strategic redundancy of evidence sources is beneficial.
Second, unless properly and continuously fine-tuned, a single intrusion detection technique may tend either to underreport electronic crimes or to overreport them (e.g., excessive false alarms). Generally, firms will find it necessary to employ multiple intrusion detection techniques in order to efficiently and effectively detect electronic crimes.

Third, experienced hackers often obscure their actions through a variety of sophisticated methods. For example, they may distribute their intrusive behavior over a number of hosts on a network in order to defeat a single host intrusion detection procedure. In such cases, intelligently selecting and fusing data from independent intrusion detection techniques, as well as the network itself, is required in order to accurately interpret this type of behavior as an electronic crime. Again, a strategic redundancy of evidence sources is helpful.

Finally, though the temptation may be great, the random and intensive search for evidence of an electronic crime is an inefficient and ineffective approach to intrusion detection. For example, if the electronic criminal can convince an intrusion detection system to continually and uselessly increase its use of computer resources, then the electronic criminal has effectively accomplished denial of service. In such a situation, computer resources are wasted and no electronic criminals are detected.

**Electronic crime detected—time for computer forensics**

In the best of all worlds, the electronic crime is detected before it is completed. Admittedly, this situation may be tricky. For example, whenever a crime is suspected, computer security personnel may need to enter the company's system through unauthorized channels, disguised as a hacker, hoping to catch any criminal in the act. Unfortunately, electronic crimes are not always detected before they are completed.

Regardless of the timing of the detection, appropriate actions should be taken by qualified professionals to successfully resolve the situation at hand. Unfortunately, many firms lack qualified computer security personnel. Even in organizations with computer security personnel, there may be a conflict of interest if the electronic crime was not prevented due to negligence on the part of such
personnel. Though a plausible alternative, many law enforcement agencies lack the technical expertise to investigate electronic crimes. Most can get the warrants and the computers, but few know how to find the evidence needed to resolve the electronic crime.

In many cases, the victim organization can best be served by retaining the services of an independent computer forensics investigator who, if desired by the company, can provide evidence to law enforcement officials and provide insight regarding the prevention or timely detection of future electronic crimes. Although hiring an independent forensics investigator may be costly, so too can be computer crime. In a recent survey conducted by the Computer Security Institute and the FBI, 74 percent of the survey respondents acknowledged financial losses due to computer crimes, but only 42 percent of the respondents could quantify the losses. Exhibit 3 shows the losses according to the type of computer crime.

The problem of how to quantify losses is a challenge. What should be included in the cost of lost data, lost time, lost business, and the hiring of a forensics expert? The higher the perceived loss to the company because of the intrusion, the greater the need to hire an expert forensics investigator.

Once the need for such an investigator is established, there are a few overriding considerations with respect to computer forensics. First, given that most electronic crimes parallel paper-based crimes, so too should the quality of investigation procedures for electronic crimes parallel those for paper-based crimes. One difficulty here is that some laws have yet to be updated to reflect the cyber nature of electronic crimes. Second, due to limited resources, decisions must be made regarding which electronic crimes should be pursued and which ones should be ignored. In some cases it may not be obvious that an electronic crime was, in fact, committed. Finally, there is a natural conflict between collecting evidential matter and getting the system fully operational. Getting the system operational too soon after an electronic crime occurs may destroy evidence necessary to appropriately resolve the crime. The danger here is that if investigations are not properly conducted, there is a very real possibility that innocent people may be found guilty of an electronic crime that they did not commit. Worse, the guilty parties remain free to commit additional crimes.

Preventing old crimes with new faces

Determined criminals will likely continue to find creative ways to invade the computer systems of businesses. Internal auditors can help their firms by ensuring that steps are taken to defend against cyber crimes. Cyber crimes are not conceptually different from paper-based schemes employed in the past. To defend against cyber crimes, intrusion detection techniques should be designed, implemented, and administered. Since intrusions are not always promptly detected, firms should establish procedures for investigation of and recovery from cyber crime. In some cases, firms should consider employing the services of a computer forensic professional. There may be "no new evil under the sun," but business models and technology rapidly change. Firms must periodically revise their information systems to prevent old crimes with new faces.