

## Incident response and fraud investigation – the role of the information technology auditor

By Willem Dirven, Anthony Samer, and David Taylor, Protiviti, Inc.

Information systems can both facilitate and detect fraud. The increasing accessibility of information systems to employees, business partners and customers, from both inside and outside the organization, heightens the vulnerability of the systems to attack and the potential for theft or misuse of confidential data.

All IT-related frauds start as an IT incident, which is an IT event that disrupts the day-to-day IT processing. Incident response is the first step: determine what happened, decide what to do about it and determine whether the incident is fraud related. If so, the next step involves computer forensics: the means by which an incident investigator retrieves and assembles evidence about a computer crime. This article discusses incident response issues and then provides detailed guidance on the role of information technology in fraud response, investigation, analysis, and prevention.

### Why is incident response so important?

Government regulations and initiatives such as Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA) of 1999 and California Law “SB 1386” are forcing businesses to pay attention to incidents that could impact the confidentiality of corporate data. These regulations call for incident response policies and procedures. Corporations in general are following this regulatory trend, particularly those who have previously experienced an incident and have realized as a result that they need to have a good plan in place.

Not every computer incident will turn out to be a fraud. However, the number of corporate network security incidents continues to climb each year with increased financial implications for companies that fall victim to an attack:

- 90% of surveyed companies detected security breaches within the last 12 months. (source: CSI/FBI Survey)

### Government Regulations and Initiatives affecting incident response

#### *Health Insurance Portability and Accountability Act (HIPAA).*

Federal law to, among other things, protect the confidentiality, integrity and availability of protected health information. HIPAA requires health-care entities to establish and maintain an Incident Response function (§164.308(a)(6)(ii)). Security portion is set at April 21, 2005.

#### *Gramm-Leach-Bliley Act (GLBA) of 1999.*

Federal law specific to financial institutions to, among other things, protect personal financial information. GLBA requires an incident response program to be developed to handle attempted and actual unauthorized access. The law went into effect July 1, 2001.

#### *California Law “SB 1386.”*

California law established in September, 2002 requiring companies to notify their customers of computer security breaches. The law applies to any online business that counts Californians as customers, even if the company is not based in California.

- 80% of surveyed companies acknowledged financial losses. (source: CSI/FBI Survey)
- 44% of surveyed companies quantified losses totaling \$455.8 million for an average of more than \$2 million per incident. (source: CSI/FBI Survey)
- Spending money on security does not reduce the number of incidents or extent of loss. However, allocating more budget dollars and resources to security does increase an organization's ability to detect loss. (source: *Information Security Magazine*)
- The knowledge required for an attacker to penetrate corporate networks is decreasing while the sophistication of attacks is increasing. (source: CERT.org)

## **Incident response steps**

After detecting an IT incident or suspected incident there are three phases of follow-up action and response:

- 1) Incident containment and damage assessment.
- 2) Collection and analysis of digital evidence.
- 3) Incident recovery and resumption of normal operations.

## **PHASE 1: INCIDENT CONTAINMENT AND DAMAGE ASSESSMENT**

### **1.1 Initial investigation**

In the first phase, incident containment and damage assessment, the immediate objective is to determine the nature and extent of the incident through network and system log analysis. It focuses on taking appropriate measures to contain the intruder, if the attack is still active.

In this phase interviews are conducted with key personnel to determine how the incident was detected and what steps have already been taken. It is helpful to interview business users to develop an understanding of the operation of the affected application or system.

Next, the investigator must determine the nature and extent of any damage or data theft, and then collect and analyze the evidence through network and system log analysis. This may include reviewing:

- System event logs. (Do any strange or unusual events appear in the logs? A data analysis tool such as ACL can help identify abnormal activity.)
- System registry. (Windows systems)
- Application logs not associated with the operating system.
- Intrusion detection system logs. (Has someone tried to enter the system using old or disabled user IDs? Have unauthorized users attempted to access the system remotely?)
- Router and firewall logs.

In the course of an investigation it may be necessary to use forensic analysis tools to gather digital evidence from PCs, servers, PDAs and other sources.

Measures taken in response to the incident will vary depending upon the specific case and typically would involve executive management and the legal department. Examples include:

- Placing tighter controls on the boundary firewall to block access to the corporate network.
- Taking the affected server(s) off the network.
- Disabling access for suspect users on the network or in an application
- Isolating the affected server(s) from the rest of the network and monitoring activity in an attempt to collect evidence.

## 1.2 Fraud incidents

An intrusion or computer security incident is not necessarily a fraud. Fraudulent activities are generally characterized as illegal or unauthorized acts that are concealed from others (through altering financial records, miscounting cash or other assets, or destroying evidence) and that benefit the fraudster – generally through sale of the stolen goods or assets. The perpetrator’s desire to conceal these activities means that frauds are difficult to observe and detect.

Some indicators of potential fraud include:

- Unusual behavior.
- Tips/complaints.
- Stale items in reconciliations.
- Excessive voids.
- Missing documents.
- Excessive credit memos.
- Common names and addresses for refunds.
- Increasing reconciliation items.
- General ledger out-of-balance.
- Adjustments to receivables or payables.
- Excess purchases.
- Duplicate payments.
- Ghost employees.
- Employee expense accounts.
- Inventory shortages.
- Increased scrap.
- Large payments to individuals.
- Unusual employee overtime.
- Write-off of accounts receivable.
- Post office boxes as shipping addresses.

As this list shows, most fraud indicators are people-based and not technology based, although technology can be used to obscure evidence or cover up fraud behavior. Most frauds are identified through observation, tips, complaints and shortages of goods or assets. Data analysis and variation analysis tools can also reveal fraudulent activities, and these are some of internal audit’s primary tools.

## 1.3 Detecting computer fraud

One of the most common ways to detect computer fraud is to log exceptions and to follow up on unusual activities in the logs. Exceptions that should be investigated include, for example:

### FRAUD FACTS

· The average fraud scheme takes about 18 months to detect. About 25% of companies hit by fraud fail to fix the problems that made them vulnerable to fraud in the first place. About the same percentage decline to notify prosecutors about frauds.

· About 30% of the time, fear of bad publicity is the stated reason for not notifying prosecutors. Certain evidentiary weaknesses and fear of counter-suits are other reasons.

· About 80% of frauds involve asset misappropriation, with cash being the target 90% of the time. Corruption in various forms accounts for about 13% of all frauds.

· The most costly and damaging frauds involve financial statements. The median loss is \$4.25 million per scheme. Legal risk and damage to the corporation’s reputation add to the cost.

- Transactions that are out of sequence, out of priority or otherwise out-of-standard.
- Aborted runs and entries, including repeated unsuccessful attempts to enter the system.
- Attempts to access applications or functions beyond a person's authorization level.

If problems are uncovered, access logs and web activity logs may provide vital clues for tracking down the person involved. Some organizations implement logging, but only on a limited basis. Data may be refreshed or overwritten too frequently for the logs to be useful for gathering evidence at a later date. Logs should be maintained for at least a few months before being erased.

Newly developed intrusion detection systems use artificial intelligence capabilities to detect unusual transactions flowing through a system. These are evolving and have the potential of providing an order-of-magnitude improvement in crime detection technology.

## **PHASE 2: COLLECTION AND ANALYSIS OF DIGITAL EVIDENCE**

Once fraud is detected, the following steps should be performed.

### **2.1 Preparation**

From the outset it is important to determine the objective of the fraud investigation. Are you going to try for criminal prosecution or for civil remedies to get your money back and dismiss involved personnel? Or are you primarily attempting to fix the problem so it won't happen again? Company officers and legal counsel will be primarily responsible for these decisions and for the decision to proceed with forensic investigation. Keep in mind, though, that an investigation may start off in one direction and end in another!

The investigator should, at the outset, identify the nature and source of the allegation and the purpose for conducting a computer forensics examination. It is important to obtain an understanding of the type of information or evidence being sought from the computer and to identify and write down string search terms. The investigator also should research any unfamiliar items, applications or operating systems that may be encountered during the analysis.

Other steps in preparing for the forensic analysis include:

- Identifying the proper size and type of storage drive to use.
- Wiping (sterilize) the storage media prior to beginning analysis. This process involves writing a series of characters over the entire physical hard drive in order to "erase" any existing data.
- Ensuring the analysis drive is fully functional without errors.
- Ensuring that the evidence locker is functioning properly.

### **2.2 Gathering evidence**

There are several tools available for gathering evidence from PCs, PDAs and other systems. Encase is a current market leader in commercial computer forensic software. Linux is a robust operating system for reading drives of various operating system types. Other open source tools are Netcat and The Coroner's Toolkit (TCT).

Forensic analysis most often begins with duplicating the hard drive of the affected computer. One duplicate drive is then analyzed for information, while the original is stored in a secure location. If the original hard drive is going to be returned to its owner before analysis and related proceedings are finalized, the first copy should be stored in a secure location, just as if it were the original item. This may happen for an in-progress fraud where a suspect still works for the company and should not be tipped off about the investigation. If the original drive is corrupted or manipulated by the owner, or a dispute arises in legal proceedings, there will be a pristine copy for reference.

It is important to maintain a proper chain-of-custody of evidence for use in future court proceedings. All original pieces of evidence should be properly marked and logged. This can be accomplished by using a chain-of-custody document to record identifying information about the item and the person it was received from. This identifying information includes:

- Date of receipt.
- Serial number of computer.
- Model number of computer.
- Serial number of hard drive(s).
- Manufacturer and Model number of internal hard drive(s).
- Signature of person delivering and person receiving the item.
- A photograph of the computer (helpful for recording the condition of the item upon receipt).

The investigator should maintain positive control over the item by locking it in a secure location (e.g. filing cabinet, safe, etc.).

Forensic analysis involves a thorough review of various aspects of the hard drive including:

- Logical file structure (all active files on the system that can be seen by a normal user or an administrator), and
- Unused file space (the portion of the hard drive that does not contain active files; however, deleted files and other data is often contained here)

### **2.3 Logical file structure review**

There are various methods available to restore the drive image and gain access to the logical file structure. The focus of the review will depend upon the type of investigation being conducted. Reviewing active files will often provide the best information. Key areas to include in this review are:

- Installed applications.
- My Documents Folder.
- Temporary Internet Files.
- Temp directories.
- Email files (Outlook - .pst; Lotus Notes - .nsf).
- Recent files viewed.
- Bookmarks.

### **2.4 Unused file space/file slack review**

Free space or unused file space is the unused portion of a hard drive. File slack is the unused space between the end-of-file marker and the end of the hard drive cluster in which a file is

stored. The most efficient way to review unallocated space is through the use of automated tools. These tools fall into two categories:

1. String search utilities – software applications that search for a designated combination of characters and report back any hits, along with the location of the find. (Note: Search terms should be carefully selected as the search results can be extremely voluminous)
2. Carving utilities – software applications that search for the header (and often the footer) of designated file types. The located files are then copied to a predetermined area, usually a subdirectory on the analysis drive. (Note: these results are also often voluminous and contain invalid files. Files obtained from unallocated space are often difficult, if not impossible, to time stamp.)

Reviewing the logical file structure and unallocated space may yield many – potentially thousands – of files to review. A manual review can take days to complete. Automated software tools can speed the process.

## **2.5 Reporting**

The investigator should work with legal counsel to determine the design and content of the report and to determine who can and who cannot receive a copy. Reports can be provided in CD or DVD in HTML format with hyperlinks to supporting information contained on the CD/DVD. This is an effective, self-contained method for concisely delivering the report and supporting information.

## **PHASE 3: INCIDENT RECOVERY AND RESUMPTION OF NORMAL OPERATIONS**

### **3.1 Recovering from fraud**

Although it may seem surprising, approximately 25% of companies hit by fraud fail to fix the problems that made them vulnerable to fraud in the first place. After an incident or investigation occurs, be sure to address the exploited vulnerabilities so the same weakness cannot be used again. A post-incident assessment on compromised systems can help identify additional safeguards to put in place. Using commercial and open source scanning software will help identify vulnerabilities in the server's operating system. The assessment should also review access rights of the network users and administrators to ensure no one has excessive privileges. It is also recommended to install additional monitoring (e.g. logging of transactions used for the fraud, logging of all transactions or logging of specific users) on the affected systems for 30 to 60 days after the incident. This will help ensure that the core weaknesses have been identified and corrected.

### **3.2 Improving fraud prevention**

Awareness of the factors that encourage computer fraud, and fraud in general, can help organizations make the right changes to reduce their vulnerability. Factors that may lead to or facilitate fraud include:

- Inadequate rewards, including pay, benefits, stock and stock options, etc.

- Failure to communicate expected standards of job-related performance or ambiguity in work roles, relationships, responsibilities and areas of accountability.
- Inadequate reinforcement and performance feedback mechanisms, such as:
  - Lack of recognition for good work, loyalty, longevity and effort.
  - Lack of meaningful recognition for outstanding performance.
  - Acceptance of mediocre performance or unacceptable on-the-job behavior.
- Failure to offer counseling when performance or behavior falls below acceptable levels
- Inadequate support or lack of resources to meet requirements.
- Inadequate operational reviews, audits, inspections and follow-ups to assure compliance with company policies, priorities, procedures and government regulations.
- Condoning inappropriate ethical norms or inappropriate behavior.
- Failure to control hostility generated by competitiveness among departments, offices or personnel.
- Failure to control bias or perceived unfairness in selection, promotion, compensation, and appraisal.
- An uncertain future (where a company faces merger, acquisition or failure, people may feel justified in "watching out for themselves").
- Inadequate standards of recruitment and selection.
- Inadequate orientation and training on security matters and on sanctions for violating security rules.
- Failure to screen and check personnel backgrounds before appointing them to sensitive positions.
- Inadequate control of the level of job-related stress and anxiety.

There are two types of controls that have been found to discourage fraud and abuse; they are internal accounting controls and computer access controls. Internal accounting controls include:

- Separation and rotation of duties.
- Periodic internal audits, including surprise inspections and computer security reviews.
- Absolute insistence that control policies and procedures be documented in writing.
- Establishment of dual signature authorities, dollar authorization limits, expiration dates for signature authorizations and check amount limits. (These authorities also should be examined on both a routine and surprise basis.)
- Offline controls and limits, including batch controls and hash totals.

Within the realm of information technology access there are a combination of technical controls to help ensure that unauthorized personnel are restricted from systems and functions that should not be available to them.

Simple password rules can help protect computer systems. Passwords should be long enough that they are difficult to guess. They should not include simple words or names of relatives that are easy to guess. They should combine upper and lower case letters, numbers and special characters, and they should be changed regularly.

Other system-based controls include:

- Compartmentalization – Restrict users to the specific files and programs that they have a job-related need to access.

- Biometrics – Use unique personal identifiers, such as a handprint or eye-scan to identify users.
- One-time passwords – Use hardware or software that generates a new password for each access.
- Automatic log off - Log out users who leave their terminal for a few minutes.
- Time-day controls - Restrict systems access to regular working hours, disallow after-hours access.
- Dial-back systems – When a user dials in to the system remotely and uses a correct ID and password, the system hangs up and dials back to a pre-established number where the approved user is standing by.
- Random personal information checks – System randomly transmits a question that only the authorized individual could answer and denies access unless the right answer is received.
- Internet authentication – This technology, which identifies a specific Internet user and sends information across the Internet securely, is rapidly evolving, as is cable-television-based broadband Internet access.
- Firewalls.

Simply following basic information security best practices also will reduce vulnerability. For example, organizations should have written policies and security rules for the use of computers and systems which are consistently applied to all systems and employees, including contractors. Employees and contractors should be instructed on security issues and should receive periodic reminders and training. Those with access to sensitive systems should be monitored closely.

Technology professionals should keep up with and close security holes in applications, firewalls and operating systems. They also should maintain fully updated virus protection and employ computer audit software to track performance.

## **CONCLUSION**

Computer incidents occur in every organization. Management should pay special attention to those computer incidents where fraud is suspected and, in those cases, should take extra care in damage evaluation, collection of evidence and especially documentation of evidence collection and handling in case court proceedings might be pursued. Management should also immediately focus on tightening controls to remediate the weakness and perform periodic additional testing to verify the operating effectiveness of any new controls to prevent future occurrences.

*Based on a presentation for the IIA San Jose Chapter and the AGA San Francisco & Silicon Valley Chapters - May 16, 2003.*

**Willem Dirven, RE** is a senior manager with the Technology Risk Services group at Protiviti, the leading firm dedicated exclusively to risk consulting and internal audit. Willem has extensive international experience assisting clients with project risk management, quality assurance, test management, software package selections, software system certifications, application controls reviews, IT efficiency and effectiveness reviews, IT strategy, and internal audits. Also, Willem's focus has been the consumer retail, wholesale, construction, software development and car & container leasing industry. Willem holds a Masters degree in Business Economics and Information Science degree from Tilburg University, The Netherlands and is a Registered EDP Auditor with the Dutch organization of Registered EDP Auditors (NOREA). Email: [willem.driven@protiviti.com](mailto:willem.driven@protiviti.com)

**Anthony Samer, CISA** is a manager with the Technology Risk Services group at Protiviti. Tony has extensive experience assisting clients in the identification, assessment, and control of technology-related business risks. He has focused on such areas as: internal technology audit, security assessments, application effectiveness and control, and project risk management. He has experience in a number of industries, but most especially the software and manufacturing sector. Anthony received a Masters degree in Business Administration from Texas A&M University, Corpus Christi. E-mail: [anthony.samer@protiviti.com](mailto:anthony.samer@protiviti.com)

**David Taylor, CISSP** is an Associate Director with the Technology Risk Services group at Protiviti and is the national practice leader for Protiviti's Incident Response and Computer Forensics practice. David has more than 10 years of experience in information systems and computer security. He is a former federal agent and Computer Crime Investigator (CCI) for NASA's Inspector General and for the United States Air Force Office of Special Investigations (AFOSI). David received a Bachelor of Science degree in Computer Science from Brockport College, New York. E-mail: [david.taylor@protiviti.com](mailto:david.taylor@protiviti.com)

Protiviti is the leading provider of truly independent internal audit and business and technology risk consulting services. We help clients identify, measure and manage operational and technology-related risks they face within their industries and throughout their systems and processes. And we offer a full spectrum of internal audit services, technologies and skills for business risk management and the continual transformation of internal audit function.

[www.protiviti.com](http://www.protiviti.com)