Realtime publishers

Monitoring, Detecting and Preventing Insider Fraud and Abuse

Dan Sullivan

sponsored by

Attachmate

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

© 2010 Realtime Publishers. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers its web site sponsors. In no event shall Realtime Publishers or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

Chapter 1: The Cost of Insider Fraud and Abuse

Advances in information technology have lead to streamlined business operations and innovative products and services. They have also created new methods for defrauding businesses, leaking private and sensitive information, and stealing intellectual property. There is a growing awareness about the need for information security. We only have to glance at a few titles streaming over technology and business news feeds to find stories of massive privacy breaches, Denial of Service (DoS) attacks, and concerted hacking attacks on specific government and business targets. The wide array of threats that businesses face do not, however, always originate from the outside.

Insider threats can be some of the most difficult to prevent and the most costly to recover from. Insiders, such as employees, contractors, consultants, and even trusted business partners, can exploit the privileges and knowledge they have acquired about business operations and practices to commit fraud, violate privacy protections, and steal valuable confidential information. Fortunately, detection and prevention practices and applications are adapting to the threats posed by malicious insiders.

This guide, *Monitoring, Detecting, and Preventing Insider Fraud and Abuse*, examines insider threats and describes tools and techniques for mitigating those threats through comprehensive, coordinated multi-system monitoring. The book consists of four chapters:

- In this chapter, we examine different types of insider abuse, such as fraud and privacy breaches, and their cost to businesses. We also briefly describe the basic requirements for effective insider abuse monitoring, such as the need to monitor multiple types of systems and correlate events across those systems.
- The second chapter considers special challenges of insider abuse, such as legitimate access, detailed knowledge of internal procedures, and the potential to tamper with security controls. The chapter highlights five key challenges to detecting insider abuse.
- In the third chapter, we describe multi-channel monitoring, application activity monitoring, and information security responses to suspicious activity. This chapter makes clear that the ability to monitor multiple applications and correlate events across diverse platforms is a key element of effective fraud prevention and detection.
- The final chapter is a roadmap to guide the reader on how to evaluate proposed solutions to insider abuse and select the most appropriate measures for a given set of business requirements.

Many of the most basic security controls, from authentication and authorization systems to firewalls and network access controls, are insufficient to protect against the threat of insider abuse. Insider threats are, by definition, threats that still exist in spite of the security controls in place to prevent unauthorized access.

These threats are not new. The problem of an unscrupulous employee "dipping into the till" is a probably as old as commerce itself. We have common practices in place to reduce the risk of insider abuse. For example, we use separation of duties to lessen the chances that a single person would be able to commit a fraudulent act. A person with access to the accounts payable system is not given access to the accounts receivable system otherwise they could conceivably create a fraudulent invoice payable to themselves as well as issue the payment for that invoice.

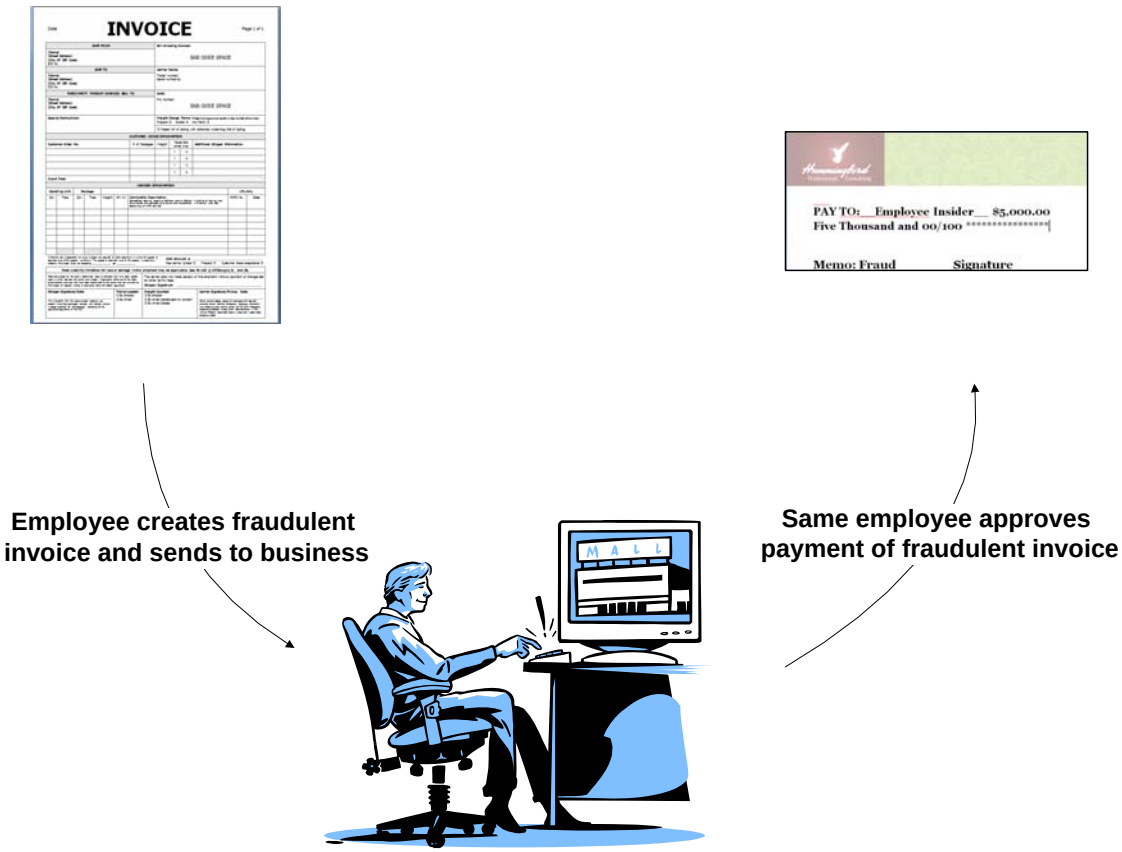

Figure 1.1: Tasks that could put the business at risk are often separated into multiple tasks executed by different employees to reduce the risk of fraud.

Today's business information systems are increasingly complex. Along with this complexity comes new opportunities for committing fraud, tampering with data, or disclosing private or confidential information.

In this chapter, we will examine examples of insider abuse and its impact on businesses. In particular, we will discuss:

- Types of insider abuse
- Cost of insider abuse to business
- Basic requirements for detecting and preventing insider abuse

We begin by looking into examples of insider abuse that illustrate the kinds of threats businesses face.

Types of Insider Abuse

Those with knowledge of business operations, access to enterprise applications and data, and a willingness to exploit that knowledge can threaten businesses in multiple ways by committing a number of crimes:

- Financial theft
- Intellectual property (IP) theft
- Sabotage
- Privacy breaches and data theft

Some of these attacks can incur direct and easily measured costs, but the impact of other crimes can be more difficult to measure. Financial theft is often easily quantified, but there are exceptions. When news of a data breach or a fine for violating regulations hits the press, customer trust and brand value can be adversely affected. Regardless of whether we can precisely quantify the full impact of fraud and abuse, there are clear consequences for businesses.

Financial Theft

A disgruntled employee looking to defraud a financial institution or other business probably has more options today than ever before. Take for example how we work with our banks.

Advances in Information Technology Exploited for Fraud

In the not too distant past, businesses would conduct commercial banking using private networks and electronic data interchange (EDI) protocols and standards. (And before that, people actually interacted in person in bank offices to conduct their financial business.) This method is well structured, comprehensive enough for many business transactions, and fairly limited in access. EDI is still used, of course, but in addition, we now have more general-purpose Web applications. A CFO can conceivably be anywhere in the world and, as long as she had access to a browser, could move funds between accounts at any time of the day.

Moving away from business-process–specific protocols and standards to general information exchange protocols used across the Internet has become a double-edged sword. Applications are more easily developed and deployed, but they are also accessible to more employees and other insiders than in the past.

Examples of Insider Financial Fraud

In spite of all the technical advances of the past decades, banks are still "where the money is." It is not surprising to see news stories of bank employees who attempt to outwit their employers and steal from the bank.

For example, an IT contractor used his insider knowledge and access to steal $2 million from his client banks by exploiting his ability to upgrade software on the bank's computers. With that kind of access, he was able to install software that posted fraudulent transactions to his accounts. He managed to get away with this for almost two-and-a-half years. (See http://www.theregister.co.uk/2010/04/30/it_consultant_sentenced/ for more details.)

In a case that combines financial fraud with privacy breaches, three Sacramento, California men, including a former bank employee, conspired to gain unauthorized access to the bank's computer systems, steal personally identifying information, and commit bank and computer fraud. One of the convicted collected customer information such as name, address, date of birth, Social Security Number (SSN), driver's license number, and credit card account details. The information was used to commit identity theft, including creating fraudulent financial instruments in the victims' names. (See http://www.justice.gov/criminal/cybercrime/thomasIndict.htm for further details.)

Banks are not the only victims of insider financial fraud. A former auditor to a California water utility attempted to transfer $9 million from the utility's bank account shortly after resigning his position. He did this by accessing two password-protected computers. Neither physical access controls nor logical access controls prevented the fraudulent transfers. (See http://www.theregister.co.uk/2009/05/26/utility_transfer_heist/ for more details.)

In all three of these examples, employees or contractors used their knowledge of the business in conjunction with their privileged access to applications to defraud the business. Clearly, existing controls are insufficient. In some cases, proper policies and procedures may not have been followed, such as in the case of the former auditor who was able to access building and computers after resigning. In other cases, existing controls may not have taken into account all the ways insiders might exploit security weaknesses; the IT contractor who continued to steal for more than two years seemed to have found such an exploit. In other businesses, it is not their funds but their ideas that lure unscrupulous employees to commit insider fraud.

Intellectual Property Theft

Imagine a computer hardware vendor who did not have to invest in engineers to design a new product or an oil company that did not have to hire teams of geologists to collect and analyze data about potential oil fields. That time and cost savings could be enormous—and therein lies the allure of intellectual property theft. Why develop the knowledge and understanding the hard way when you can have it for a fraction of the cost in very little time? A few different scenarios seem to play out in intellectual property theft:

- An employee steals intellectual property, such as a client list, and starts a competing business
- After stealing trade secrets, an employee sells them to a competitor
- An employee steals intellectual property in order to secure a position with a competitor

As the following examples show, bankers, auditors, and IT consultants are just the start of the list of potentially abusive insiders.

Consumers are eager for display devices that provide high-quality images and consume little power. Liquid crystal displays (LCDs) are popular but organic light emitting diodes (OLEDs) devices can be lighter, thinner, and provide deeper contrasts. One can imagine that developing OLED technology and dealing with thermal evaporation in a vacuum, electroluminescent conductive polymers, and other chemical and material science issues is difficult to say the least. One chemist for an international chemical company tried to advance his career by stealing trade secret information on improving the longevity and performance of OLEDs. He stole samples and documents describing chemical processes that could have been used to jump start development of a competitive product. (For further details, see http://www.justice.gov/criminal/cybercrime/mengPlea.pdf.)

In another case, a low-level engineer managed to steal $1 billion (yes, that is with a 'b') worth of intellectual property. The engineer resigned his position working for a major microprocessor manufacturer to go to work for a competitor. While still employed by the victim and supposedly using remaining vacation time, he went to work for the competitor. His access to the victim's computer systems were not terminated until a week after he started with the competitor. During this period, the engineer downloaded 13 "top secret" (internal classification) documents from his soon to be former employer. The documents contained details on the process for developing next-generation microprocessors. There were multiple controls in place to prevent IP theft:

- Physical access restrictions
- Authentication and authorization controls on computer systems
- Use of encryption in the document management system
- Restriction on remote access through the use of a virtual private network (VPN)

Even though the victim company seems to have implemented security best practices, an insider was able to circumvent these controls and steal essential intellectual property. As in the earlier bank example, we have a case where an insider can avoid detection and prevention mechanism of common security measures. (For more details on this case, see http://regmedia.co.uk/2008/11/06/amdintelpaniindictment.pdf.)

Sabotage

Revenge, like greed, is motivation for insider abuse. A disgruntled insider with the right combination of knowledge and access can wreak havoc on business operations using only a handful of scripts. Sabotage of computer systems can come in many forms:

- Deleting or altering data
- Disabling system logging
- Destroying or corrupting backup files
- Denying administrative access to systems
- Altering the functionality of legitimate programs

Take the2008 case of a disgruntled IT professional at a mortgage company. According to an indictment, shortly after being fired from a mortgage company, a former IT administrator planted a series of scripts that would execute a few months in the future and destroy data on all production, test, and development servers at the company. Known as logic bombs, these scripts could have disrupted operations for a week and cost the company millions of dollars to recover had they not been discovered and disabled.

The former employee's position gave him access to servers throughout the organization. Between the time he was notified of being fired and his access privileges were actually terminated, the former IT administrator embedded several malicious scripts inside a legitimate application. The script included commands to:

- Copy malicious files to a server and begin running them
- Block monitoring programs to mask the activities of this script as it executed
- Disable administrative logins to the administrative and backup production servers
- Remove root password access
- Overwrite data on the server with zeros
- Disrupt software supporting high availability

The script would then copy itself from initial target server to the other 4000 servers in the company. Taking a practice from high-reliability design, the former employee designed the scripts to repeat the process from another administrative server in the event some of the servers were not available during the initial attack.

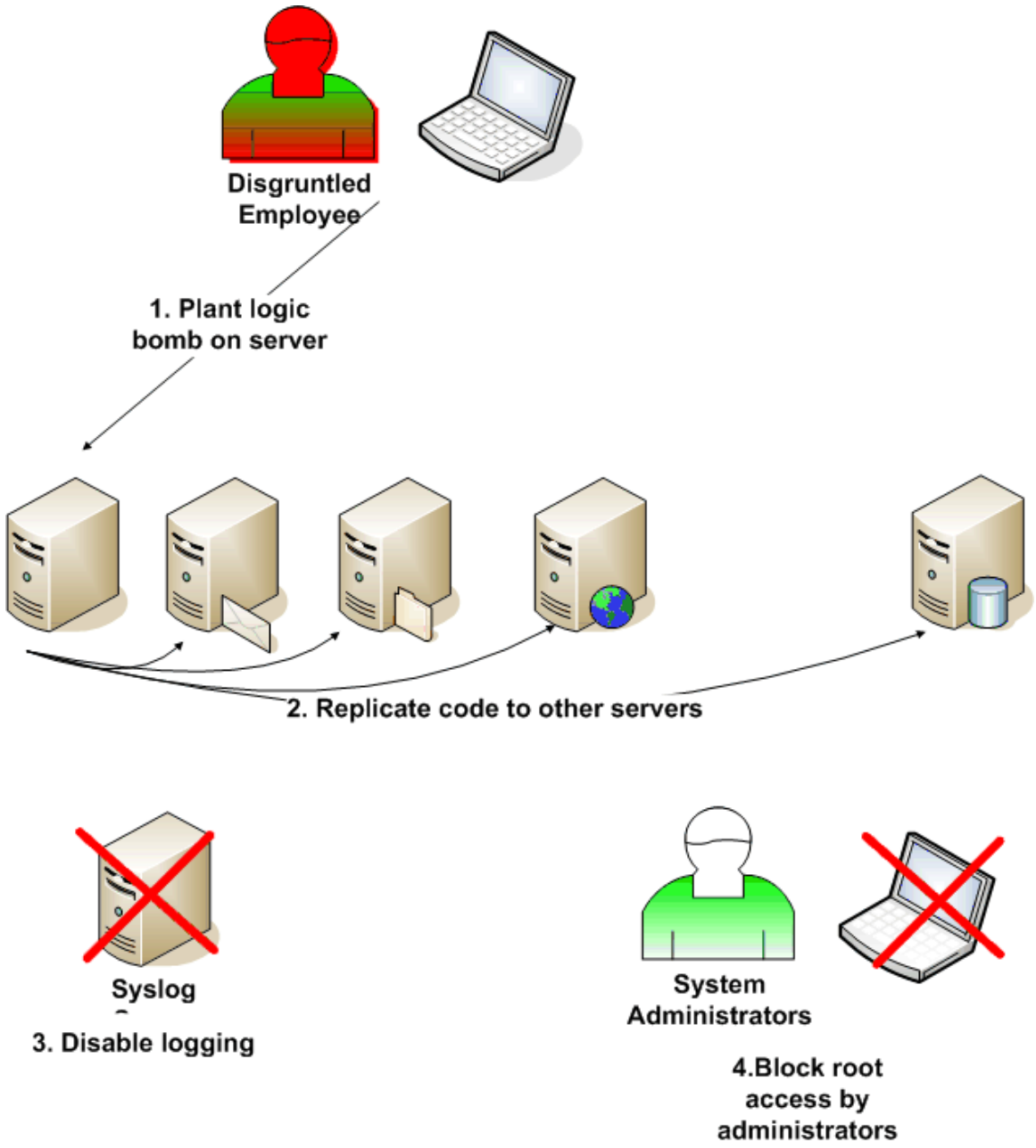

Figure 1.2: Common elements of logic bomb attacks include installing malicious code, blocking logging, and preventing administrative access by other privileged users.

The company was fortunate that an engineer came across the scripts several days after the former employee was terminated. (For more details on this case, see http://www.theregister.co.uk/2009/01/29/fannie_mae_sabotage_averted/.)

Other examples of insider sabotage include:

- A former IT consultant who cause $1.2 million (Australian) in damages to his former employer by deleting more than 10,000 user accounts on government servers. The man was trying to demonstrate security vulnerabilities in the systems; he was also drunk and upset that his fiancé had broken off their engagement. (http://www.theregister.co.uk/2009/03/13/nt_hack_convict/)
- A subcontractor to the IRS planted a logic bomb on three servers prior to being dismissed. The scripts included commands to disable system logs, delete files, and overwrite the malicious code to prevent detection. (http://www.justice.gov/criminal/cybercrime/carpenterPlea.htm)
- A former network administrator changed passwords on a city FiberWAN and refused to disclose the new passwords to administrators leaving the city without administrative control of the network for 12 days. (http://www.computerworld.com/s/article/9176060/Childs_found_guilty_in_SF_network_password_case).

These examples of insider abuse by trusted IT professionals demonstrate how readily disgruntled employees with knowledge and access can inflict significant damage. Another form of insider abuse with consequences for compliance and brand damage are privacy breaches.

Loss of Privacy and Data Thefts

The ease with which personal information is collected, disseminated, and stored has developed along with growing concerns for the need to protect privacy. As early as 1995, the European Union (EU) began implementing a data protection initiative; and the United States passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996, which includes regulations governing personal health information. Protections for financial information were established by the Gramm-Leach Bliley Act (GLBA) of 1999. Many states have also passed legislation defining privacy protections for consumers, such as California's California SB-1386 passed in 2002. Compliance with privacy regulations has become a significant concern for businesses; remaining in compliance is especially challenging when companies have insiders with access to protected information.

Privacy breaches tend to fall into two general categories:

- Broad privacy breaches in which a large number of customer, client, or patient records is disclosed in an unauthorized manner.
- Targeted privacy breaches, otherwise known as VIP snooping, in which detailed information about a well-known person's personal, health, or financial information is disclosed in an unauthorized way.

Both types of privacy breaches are vulnerable to insider abuse.

Insider Abuse and Broad Privacy Breaches

Access to tens of thousands of records with personal, financial, and health information can prove to be too tempting for some to resist. Sometimes greed, fueled by hopes of selling confidential information for lucrative gains, motivates insiders to abuse their privileges. This is especially problematic when financial information is involved. Here are a few telling examples.

In one case, a call center employee for a major US bank stole private customer information in an attempt to establish fraudulent credit card accounts. The employee attempted to sell name, date of birth, and other personal information in return for a share of gains from credit card fraud. The incident could have potentially cost the bank $1.3 million. (See http://www.theregister.co.uk/2010/06/08/bank_insider_data_theft/ for further details.)

A financial analyst for a subprime division of a major mortgage company sold up to 2 million records containing personal and financial information of mortgage applicants. The analyst sold batches of approximately 20,000 records for $400 to $500 each. The perpetrator was able to continue for about two years, in part because he used a computer without the same security controls as the others in the office. (See http://articles.latimes.com/2008/aug/02/business/fi-arrest2 for further details.)

Each of the victim companies no doubt had security controls in place, but the malicious insiders were able to at least begin the process of breaching private information and in at least one case were able to continue for almost two years. The mortgage company employee was probably more familiar with the weaknesses in one office computer than the IT staff and that proved to be a critical piece of information for carrying out his crime. Other privacy cases show that targeted attacks on individual's private information are also a known risk.

Targeted Attacks and VIP Snooping

Given the number of magazines and gossip columns dedicated to the lives of famous and popular persons, there must be sizeable demand for even the slightest bit of private news about those individuals. It is little wonder that some employees with access to private information about celebrities are tempted for their own interest or for profit to breach the privacy of others.

A California-based medical center was recently fined $130,000 for a violation of a patient's privacy. On seven occasions, the medical records of a single patient were accessed in unauthorized ways from five doctors' offices, a credit agency, and by a medical center employee. The medical center discovered the violation through its monitoring of high-profile cases. (See http://www.enloe.org/about_us/news_and_publications/2010/enloe_protests_health_privacy_citation.asp for further details.)

This case shows just how difficult it can be to protect the privacy of individual customers when many types of users have access to data from multiple systems. It is not, however, the only instance of such a breach. *The New York Times* has reported on multiple instances where popular actors and singers have had their privacy violated by employees at medical facilities, possibly leaking the information to the press. (Tara Parker-Pope "More Celebrity Snooping by Hospital Workers" at http://well.blogs.nytimes.com/2008/04/03/more-celebrity-snooping-by-hospital-workers/.)

Business data and assets from personal healthcare information to financial assets to intellectual property are subject to insider attacks. Employees, contractors, and business partners may all have legitimate requirements for access to applications and data. Most will use those privileges in a manner consistent with the way they are expected to be used, but as the previous intellectual property case demonstrates, even a single instance of a breach of that trust can have significant costs.

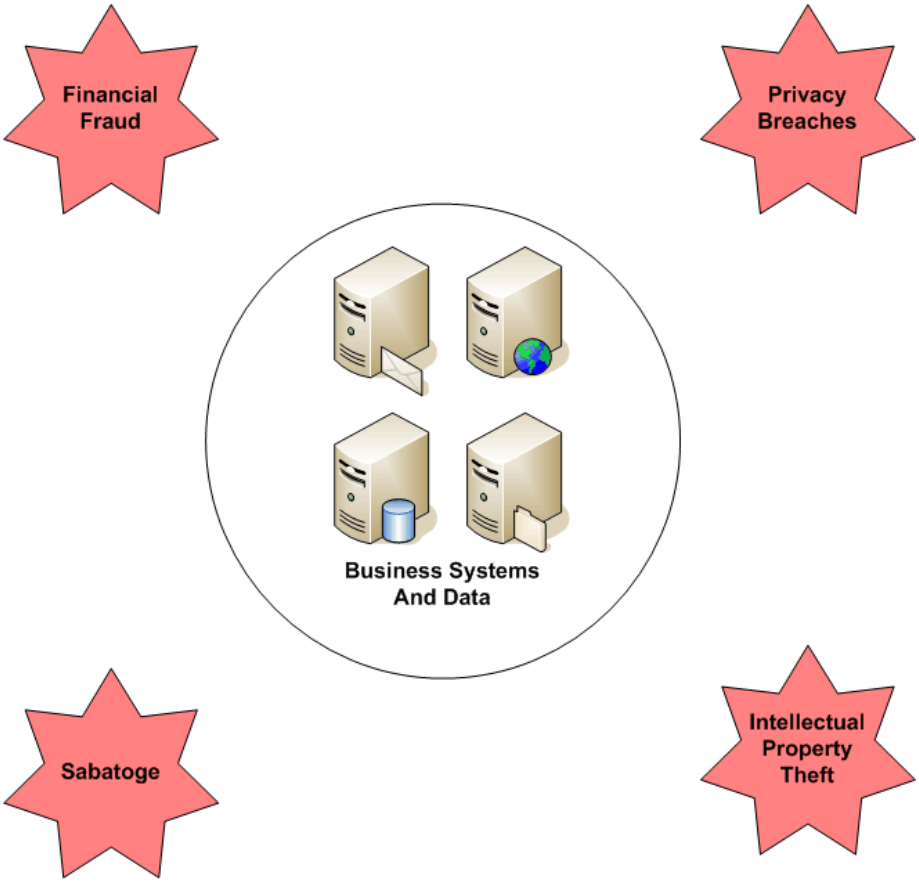

Figure 1.3: Business systems and data are continually subject to four types of insider threats.

The Cost of Insider Abuse

It is clear from the previous examples that insider abuse can have clear and immediate consequences for the corporate bottom line. In addition, there are costs associated with violating regulations and the potential for less easily quantified damage to brand and reputation. We will consider each of these.

Financial Losses Due to Insider Abuse

Financial losses come in several forms, some of which are direct and some are more indirect. Direct financial losses, including costs of recovering from an insider abuse incident, include:

- Funds stolen directly by the malicious activity, such as wiring funds from corporate accounts to an attacker-controlled account
- Credit extended to a fraudulent customer account set up by an insider
- Payments to customers, clients, or patients who are victims of privacy breaches
- Cost of restoring systems and data destroyed by a disgruntled employee who left a logic bomb on the corporate network, including additional labor costs to restore systems and verify data up to the point of the attack

Financial losses may be less direct but they ultimately affect the bottom line. These indirect costs include:

- Opportunity cost of missed investments because funds were not available due to insider fraud
- Interest on funds borrowed to meet short-term expenses that would otherwise not be covered because funds were stolen by an insider
- The cost of post-incident response and forensic investigations

Ironically, additional security investments before the attack might deter or discourage the types of insider abuse before there is significant damage. As is often the case, the cost of prevention is less than the cost of the cure. These direct and indirect costs may be only the beginning if the incident demonstrated insufficient compliance with regulations governing corporate management or privacy protections.

Compliance Violations

Today's business world is more complex and interconnected than ever before. Private investors and institutions make major decisions about how they allocate their investments based on corporate earnings reports and other financial and management information provided by businesses. If that data cannot be trusted, the investment markets will not function. It was not long ago that names such as Enron, Adelphia, and WorldCom became almost synonymous with corporate accounting scandals. To prevent a repeat of such corporate management failures, regulations were created to require firms not only to provide accurate information but also to protect the information systems that manage corporate accounts.

At roughly the same time, major accounting scandals were prompting new financial controls and growing concerns about privacy were driving the adoption of privacy regulations around the globe and at jurisdiction levels ranging from states to nations and transnational organizations. The best known of these regulations that also have consequences for insider abuse incidents are:

- HIPAA
- Payment Card Industry (PCI) Data Security Standards (DSS)
- Sarbanes-Oxley (SOX)
- GLBA

Each of these address different types of protections which may be violated during insider abuse incidents.

HIPAA

HIPAA defines levels of protection that need to be in place when managing, distributing, or storing protected health information. These regulations apply to businesses in the healthcare industry and include hospitals, clinics, doctor's offices, health insurance companies, and healthcare clearinghouses. The regulation covers what types of healthcare information are considered private and who it can be disclosed to. Another part of the regulation specifies administrative, physical, and technical safeguards required for business processes and information systems used to process protected healthcare information. Penalties for violations can be as high as $1.5 million per violation.

> **HIPAA Enforcement**
>
> HIPAA enforcement has received a boost recently with additional funds and a shifting of security enforcement responsibilities. See Niel Versel "OCR Stepping Up HIPAA Privacy, Security Enforcement" at http://www.fiercehealthit.com/story/ocr-stepping-hipaa-privacy-security-enforcement/2010-05-17.

PCI DSS

The PCI DSS is an industry regulation specifying security controls to mitigate the risk of credit card fraud and information theft. The regulations include policies on:

- Maintaining a secure network
- Protecting cardholder data when stored or transmitted
- Implementing a vulnerability management program to maintain systems security
- Implementing access control methods to limit access to cardholder data
- Monitoring network and systems and testing them regularly

As this is an industry standard, there are no government penalties for violations, but businesses that fail to comply may suffer restrictions on their use of payment card services. The failure to comply with PCI regulations may also indicate failure to comply with government regulations, which in turn, could result in fines and penalties.

SOX

SOX was passed in direct response to corporate accounting scandals. Much of the regulation addresses corporate governance and financial reporting. One section is of particular interest to IT professionals: Section 404. Section 404 regulates the need for internal controls over how financial data is collected, managed, and reported. Companies are responsible for:

- Having controls in place to prevent misstatements on financial reports
- Risk assessment with regards to information management systems
- Controls on the financial reporting process

Obviously, if insiders are able to manipulate internal records, commit fraud, and hide their activities, controls are insufficient to protect the integrity of a company's financial system.

GLBA

GLBA applies to financial institutions and includes protections for consumer privacy. Financial institutions are required to provide customers with details on what information is collected, how it is shared with other institutions, and what safeguards are in place to protect that information. Requirements include:

- Access controls on systems containing customer data
- Use of encryption
- Physical access controls
- Monitoring for abuse, attacks, and intrusion
- Incident response plans

The examples described earlier of bank employees selling account information demonstrate the kinds of incidents that constitute violations of GLBA. The cost of compliance violations to businesses will vary according to the type of violation, the level of enforcement, and other factors regulators may take into account, such as past violations, negligence, and response to incidents.

Brand Damage

Companies can damage their reputations when insider abuse incidents become public. Would customers trust a bank that cannot trust its own employees not to sell customer information at a rate of pennies per record? How would investors react to a significant loss of intellectual property because a company's IT department did not adequately monitor networks and applications? Brand damage can adversely affect a company from a customer and revenue perspective as well as from an investor and market capitalization perspective.

Insider abuse can impose significant financial and nonfinancial costs on a company, including direct costs of fraud, the expense of recovering from sabotage, and lost competitive advantage due to intellectual property theft, as well as the less easily quantified but just as real brand damage. Insider abuse is an established risk and, like other known security risks, requires a well-designed mitigation plan to protect the business.

Basic Requirements for Monitoring and Detecting Abuse

Commonly used security controls, such as access controls, intrusion prevention systems, and anti-malware systems are critical to keeping outsiders away from a business' computer systems and data. Taken separately or together, none of these security controls provides enough protection against insider abuse. Some of the examples of insider abuse come from banks and high-tech companies that probably have some of the most comprehensive security controls across a range of industries. Old security models such as perimeter defenses and the "block and tackle" approaches of access controls and intrusion prevention are not designed to protect against insiders.

Insider abuse requires us to deal with an apparent contradiction. We grant insiders access because we trust them but we still need to protect against them. The problem is that although companies can trust their employees in general there is some small probability that one or more of those employees will exploit that trust for their personal gain. If the cost of insider abuse was as small as the probability that a specific employee will commit abuse, we might be able to absorb the cost; unfortunately, that is not the case. A single incident can have damaging consequences for a company. To address the threat of insider abuse, we need new types of security controls including the ability to monitor multiple types of system and to correlate activities across the enterprise.

Monitoring Multiple Types of Systems

Distributed systems are commonplace. Businesses continue to use mainframes for high-volume, core business processes. Web applications are opening opportunities for delivering new types of services. Databases collect, store, and manage data from multiple applications. Specialized servers are used throughout organizations to provide services such as document management, file transfer, email, and other collaboration services. An insider attack can involve all of these different types of systems.

Imagine how an insider might use knowledge of a business process to commit fraud. The insider knows how one Web application is designed to create new customer accounts through a multi-step process. The insider might bypass the first steps of the process that validate an application and insert data into a queue of applications that are processed by a mainframe job. The mainframe programmers assume anything in the queue must have been validated, so all applications, including the fraudulent ones, are accepted. The insider then uses the bogus customer account to order several expensive items. With some further tampering, he inserts a payment transaction into the database supporting a customer Web application. The bogus payment is credited to the account after which the insider creates a return order which in turn generates a refund check to the "customer."

In spite of the obvious problems these transactions would create on reconciliation reports, this fictional example shows how an insider can use multiple systems to commit fraud. Complex business processes do not always have well-defined reconciliation procedures and even when they do, small discrepancies may not warrant detailed investigations. An insider who understands the parameters of the review process can effectively "fly below the radar."

In later chapters, we will go into further detail on the need to monitor mainframes, Web applications, databases, file servers, and other servers.

Correlation of Activities

One of the challenges with monitoring multiple systems is correlating events across those systems. For example, an event on an application server might indicate that a customer record is being updated. Shortly after that, there is a change to the database and a customer record is updated. It is reasonable to assume that a Web application called a service on the application server that in turn executed an update procedure on the database. Now consider an event in which a record is added to a queue for processing transactions but there is no corresponding event in any of the applications that generate new queue entries. This may be a case of someone purposefully bypassing the normal business process. Only by monitoring all the systems involved in business processes, can we collect the data we need to monitor insider activity.

In addition to correlating events from multiple systems and multiple activities, we need to carefully account for the timing of events. One of the most basic problems we have in correlating events is the lack of a universal time reference. Each system will use its own internal clock to timestamp events. If all monitored computers are running time synchronization services, such as Network Time Protocol (NTP), this is less of a problem. With synchronized times, we can use event timestamps to order events and measure the time difference between events. Anomalies in event times can be an indication of tampering. For example, if event A usually occurs 1 second after event B but sometimes occurs 8 seconds after A, the latter may be an indication of tampering (for example, additional code is executing in the process, perhaps covering tracks). (It may also be an indication of a performance problem but such problems would likely be consistent across many transactions).

This type of monitoring introduces the problem of erroneously classifying a legitimate event as malicious. These are known as false positives. For example, the transaction that takes 8 seconds instead of 1 to complete may have been due to a network error, an unrelated error on a server that delayed processing, or some other unexpected but not malicious event. Event monitoring across systems and across time is a powerful method for detecting insider abuse, but we must remember it is based on patterns and statistical inference. Sometimes we get it wrong. In later chapters, we will delve further into the challenges of multi-system monitoring and ways to address those challenges.

Summary

Insider abuse can take many forms: financial fraud, privacy breaches, intellectual property theft, and sabotage are some of the most costly. Each of these different types can result in substantial costs to businesses that range from the direct cost of fraud to the cost of remediating sabotage to the cost of brand damage when the press publishes details of the incident. Commonly used security controls that are designed to keep outsiders out are insufficient when dealing with insiders. By definition, we are dealing with individuals who have been entrusted with access to business systems and have knowledge of business processes. Detecting and preventing abuse by these individuals will require a new level of monitoring and control.