

An Introduction to Insider Threat Management

infoLock Technologies

EXECUTIVE BRIEFING

Insiders — employees, contractors, consultants, and vendors — pose as great a threat to an organization’s security posture as outsiders, including hackers. Few organizations have implemented the policies, procedures, tools, or strategies to effectively address their insider threats. An insider threat assessment is a recommended first step for many organizations, followed by policy review and employee awareness training.

INTRODUCTION TO INSIDER THREAT MANAGEMENT

Who is more dangerous: the robber trying to break into the bank or the disgruntled employee with the keys to the safe? Both individuals pose significant security threats and could commit serious crimes, but the employee — unlike the criminal — is extremely difficult to identify, monitor, and protect against. The bank can install sophisticated locks, bulletproof dividers, and closed circuit cameras to deter thieves from the outside, but can they determine who the thieves are on the inside?

This challenge is at the heart of Insider Threat Management (ITM), an emerging focus area of information security and operational risk management that deals with the security threats posed to organizations by “insiders,” the trusted individuals who possess intimate knowledge of internal operations and processes, or have access to an organization’s sensitive data and resources. It is a systematic approach to assessing, monitoring, and mitigating insider threats.

This white paper provides a comprehensive overview of insider threat management to include a brief history of computer crime and hacking, analysis of significant insider threat types, legal and human resource implications for organizations, and practical strategies for assessment and mitigation. Additionally, it discusses the need for senior management buy-in and awareness training and education.

The Evolution of Information Security

Although modern digital computers emerged before World War II, and personal computers (PCs) in the late 1970s, it wasn’t until the widespread

35 commercial growth of the Internet in the 1990s that unethical or criminal “hackers” became a primary security concern for information technology professionals and the organizations that employ them.

40 Over the last 10–15 years, organizations have spent billions building strong perimeter defenses to protect their data from hackers and other outside attackers. Organizations now enjoy a dizzying array of “perimeter security” mechanisms from which to choose, including anti-virus software, 45 firewalls, intrusion detection and prevention systems, anti-spam, logical and physical access control systems, malware/spyware protection, email and database encryption, and Web application security systems.

50 On average more than 75 percent of corporate information security budgets are directed toward protecting against outsiders*, even though the 2005 Computer Security Institute/FBI Computer Crime and Security Study found that insiders were responsible for just as many incidents as outsiders. 55

Who is a Hacker?

60 So why are we so concerned with outsiders? The reality is that outsiders have inflicted serious damage, and organizations need to protect themselves from the nefarious individuals who seek to steal sensitive information or maliciously damage critical resources. However, it is also true that from a psychological perspective, it is more common, perhaps 65 easier, to fear and mistrust outsiders than it is to be concerned with insiders and the security risks they pose. Our natural fear of the unknown has led to greater media coverage about hackers, and has placed greater emphasis on technology tools that defend against outside threats.

70 A hacker is generally understood to be a malicious or criminally minded outsider who seeks to cause damage to organizations or individuals for financial gain or personal notoriety. These individuals, who are more accurately referred to as “blackhat hackers” to differentiate them from general technology enthusiasts known as “whitehat hackers,” are responsible for the release of viruses, worms, and trojan horses, propagation of malware

and spyware, Denial of Service (DoS) and DNS poisoning attacks, spam and phishing campaigns, 80 and social engineering† exploits on unsuspecting human targets.

Media accounts of computer criminals and hacker culture have fueled the public imagination. Recent news stories have focused on organized hacker rings 85 in Russia, Africa, and Southeast Asia that have caused millions of dollars in damage. The 1995 arrest and conviction of Kevin Mitnick for social engineering and hacking remains one of the most celebrated and controversial cases of its kind, lending support 90 to the popular opinion that hackers are among the most dangerous non-violent “white collar” criminals in society.

The personal risks posed by hackers to private citizens are well known and widely discussed. Public and private organizations; federal, state, and local government agencies; the military; and all types of corporations now understand that hackers threaten their operations, and have therefore taken significant steps to secure sensitive computing systems from 100 these external threats.

When it comes to security, however, is a hacker more dangerous than a trusted insider? The research in this area makes clear that while hackers are responsible for many security breaches and attacks, 105 insiders cause more security problems. In a recent FBI study, nearly half of all respondents said they had experienced intrusions from within their organization‡. A 1998 survey conducted jointly by the Computer Security Institute and the FBI found that 110 the average cost of successful computer attacks by outside hackers was \$56,000. By contrast, the average cost of malicious acts by insiders was \$2.7 million.

† Social engineering refers to a hacking technique in which an organization’s insiders are targeted for sensitive information, which is later used to launch technical attacks and exploits.

‡ The 2005 FBI Computer Crime Survey was taken by 2,066 organizations in Iowa, Nebraska, New York, and Texas in Spring 2005. The report is designed to “gain an accurate understanding” of computer security incidents. The 23-question survey addressed such issues as the computer security technologies enterprises use, what kinds of security incidents they’ve suffered and what actions they’ve taken. The survey is not the same as the CSI/FBI Computer Crime and Security Survey, which has been conducted for several years and has a somewhat different focus, method and restricted number of respondents.

* Yankee Group, 2006.

THE INSIDER THREAT

Who is an insider? Simply stated, an insider is anyone who has intimate knowledge of internal operations and processes, or trusted access to sensitive data and resources. The term insider is often narrowly defined as part- and full-time employees. While employees certainly comprise the bulk of insiders, organizations often fail to consider the security implications caused by consultants, contractors, vendors, and partners — entities who also possess inside knowledge of the organization or trusted access to data and network resources.

Failing to recognize this security threat has already had serious consequences for many organizations, especially in light of two major business trends — outsourcing and remote connectivity. Outsourcing key corporate functions to low-cost providers, and employee access to corporate resources from around the globe, have decreased costs and increased efficiency. However, they also have led to the transmission and storage of sensitive data beyond the corporate firewall, extending the security perimeter to places beyond an organization's control.

For example, few organizations question the security posture of a third-party vendor or the financial and criminal records of employees at vendors who process payroll or store backup data tapes. Unfortunately, once sensitive information leaves the organization's perimeter, the definition of who is an insider must be broadened.

Another common mistake in defining insider threats is limiting focus on malicious insiders. Failing to recognize the threats from insiders' unintentional or accidental actions also has led to a number of high-profile security breaches. According to the 2005 FBI Computer Crime Survey, trusted insiders accounted for 52 percent of all security breaches in 2004, with the majority of reported incidents attributed to otherwise well-meaning employees' unintentional mistakes and careless behavior. Malicious insiders, including employees who meant to cause damage or to steal sensitive information, were responsible for a much smaller percentage of security breaches and incidents.

Some notable insider security breaches committed by malicious insiders include the following:

- In July 2006, three Coca-Cola employees were charged with attempting to sell confidential corporate trade secrets to Coke's main competitor, PepsiCo. 165
- In May 2005, Wachovia and Bank of America were forced to notify more than 100,000 customers after nine people, seven of whom were employees, were caught stealing and selling sensitive data about bank customers. 170
- A computer programmer at the Georgia Technology Authority was arrested in April 2005 for downloading and stealing 465,000 files on Georgia drivers during off-hours. Investigators never determined what the former employee was going to do with the sensitive data, which included social security numbers. 175

The Wachovia and Bank of America employees are clearly criminals and can be classified as such, but it's not just these malicious insiders that cause risks; often an organization's best employees make significant security blunders and mistakes. These mistakes are the result of employees cutting corners due to laziness or frustration with "annoying" or "inconvenient" security policies. Not surprisingly, insiders' efforts to increase productivity by circumventing security policies can lead to serious security breaches. 180

Some notable insider security breaches committed by well-meaning insiders who made mistakes or showed poor judgment include the following: 190

- In May 2006, the names, addresses, and social security numbers (SSNs) of more than 26.5 million U.S. military veterans and active duty personnel were lost when a laptop and external hard drive were stolen from the home of a Veterans Affairs analyst. The laptop and hard drive were subsequently recovered with no apparent loss of data. 195
- Although not disclosed until June 2006, in February 2006 a laptop containing the names and credit card numbers of 243,000 Hotels.com customers was stolen from an Ernst & Young auditor working at the company. 200
- In October 2005, a Wilcox Memorial Hospital employee in Kauai, Hawaii, reported a USB thumb drive — containing information on 130,000 former and current patients — had been lost and was presumed stolen. 205

TABLE 1 Daily Activities and Security Incidents

Activity	Potential Benefit	Security Threat
Instant messaging	Faster communication among employees, and with vendors and customers; reduces overhead on telephone and email systems	Spyware/malware/virus infection from outside, leakage of sensitive information, decrease in employee productivity due to "personal" use
Email	Faster communication among employees, and with vendors and customers; reduces overhead on telephone and email systems	Spyware/malware/virus infection from outside, leakage of sensitive information, decrease in employee productivity due to "personal" use
Use of USB thumb drive	Convenient transfer of large amounts of data, small size, easy to use with today's 'plug and play' operating systems, inexpensive	No differentiation between authorized and "rogue" devices, no audit or logging of data on devices, no centralized control, leakage of sensitive data, infection from outside data brought in to network on devices
Accessing network shared drives	Centrally managed data storage, can be made highly available and archived securely	Users access sensitive files or folders that should be "off limits" to them, leakage of data outside network
Use of smartphone or PDA device	Mobile productivity, enabling employees to work remotely	Physical loss of device leads to data loss/theft, data transmissions may be intercepted or "sniffed"

Studying the Insider Threat

While there have been few comprehensive studies of insider threats, perhaps the most notable is the 2004 Insider Threat Study (ITS) conducted by the U.S. Secret Service and CERT Coordination Center/Software Engineering Institute at Carnegie Mellon University. The incidents examined in the ITS are incidents perpetrated by insiders (current or former employees or contractors) who intentionally exceeded or misused an authorized level of network, system, or data access in a manner that affected the security of the organizations' data, systems, or daily business operations.

Incidents included any of the following actions committed against any information system, network, or data for which the attacker did not have authorization:

- compromise
- manipulation
- unauthorized access
- exceeding authorized access
- tampering
- disabling

The cases examined also included any in which there was an unauthorized or illegal attempt to view, disclose, retrieve, delete, change, or add information.

Good Employees Often Make Bad Decisions

235

How do you correct the careless behavior or unintentional mistakes of an otherwise well-meaning employee? You can encrypt the data on an employee's laptop, install secure email software, or implement a draconian security policy, but is that an appropriate response? Security has always been at odds with productivity, and finding the right balance is difficult. The answer will depend on your industry and the sensitivity of your data, but can only be determined after careful analysis.

It is important to note that mistakes and mishaps do not mean employees are "bad" or have malicious intent. In fact, few companies can afford to fire good employees that make a few bad decisions.

For example, employees engage in numerous daily activities that increase efficiency and productivity, but can result in significant security incidents (see Table 1).

THE STOLEN LAPTOP EXAMPLE

255

An otherwise model employee may take a company laptop computer home for the weekend, against policy, in order to get a report done on time. That employee may carelessly leave the laptop in the backseat of his car, in plain view, in a position to be

stolen. If the laptop is stolen, the company may be exposed to lawsuits, civil fines and penalties, erosion of stockholder trust, and reputation damage, not to mention the impact on private individuals and customers whose personal data was stolen.

The problem lies not in the intentions of the employee but in how little visibility the company and its management have into the employee's actions. Executives could easily have been caught flat-footed by the laptop theft.

Inside the Mind of the Malicious Insider

It is important to recognize the danger of non-malicious employee behavior, but clearly all insider breaches are not accidental. In "Inside the Mind of the Insider," an article about the psycho-social characteristics of malicious insiders, authors Eric Shaw, Jerrold Post, and Keven Ruby identified six personal characteristics with direct implications for risk:

- Sense of entitlement
- History of personal and social frustrations
- Computer dependency
- Ethical flexibility
- Reduced loyalty
- Lack of empathy

Sense of entitlement. A key trait of many of the attackers was a sense of personal entitlement, that one is special and owed corresponding recognition or privilege. The Shaw study found that entitlement feelings were frequently reinforced by the employer. When combined with a preexisting anger toward authority figures, this sense of entitlement motivated a desire for revenge, in reaction to perceived slights or setbacks.

Personal and social frustrations. Professor R. Caldwell, a computer scientist who conducted separate studies in 1990 and 1993, identified that some individuals exhibit "revenge syndrome." These individuals often have a history of personal and social frustrations, often including childhood abuse and neglect. They tend to exhibit anger, alienation from authority, fewer social skills than peers, and an inclination to "strike out at the system."

Computer dependency. In the Shaw study, online activity significantly interfered with or replaced direct social and professional interactions for many of their subjects. According to psychologists, computer-addicted individuals are more likely than nonaddicted users to be aggressive loners who make poor team players. They report their primary interests as exploring networks, breaking security codes, hacking into computer systems, and challenging and outfoxing security professionals.

Ethical flexibility. Many of the subjects whose cases were studied by Shaw reportedly did not view their violations as unethical; some even viewed them as justified under the circumstances. These subjects appeared to lack the moral inhibitions that prevent others from committing such acts. This finding is consistent with earlier research on ethical boundaries within the "information culture" conducted by S. Harrington and published in 1995. Harrington's findings indicate that approximately 7 percent of computer professionals do not object to cracking, espionage, or sabotage. Their rationale is that an electronic asset is fair game for attack if it has not been sufficiently secured by the company.

Reduced loyalty. The subjects in the Shaw study appeared to identify more with their profession or computer specialty than with their employer. This finding is reminiscent of a study of computer fraud conducted by the U.S. Department of Health and Human Services in 1986, which found that computer programmers who committed fraud felt more loyalty to their profession than to their employer.

Lack of empathy. An employee's disregard for the impact of his or her action on others, or inability to appreciate this impact, has been noted consistently by investigators. Likewise, many of the subjects in the Shaw study lacked empathy. This characteristic is magnified by the nature of cyberspace, where the effect of events is muted by the lack of immediate apparent consequences.

STRATEGIES FOR MANAGING INSIDER THREATS

Insider threat management is an emerging focus for risk management and information security professionals, and those responsible for protecting an

organization's reputation and public standing. Effective insider threat management requires an organization to locate and classify its own sensitive data, systems, and resources, and to remain continuously vigilant regarding employee behavior and associated risks.

Technical solutions alone cannot always detect or discover insider threats or address them appropriately. Insider threats are personnel threats first and foremost, not technical threats, and human beings require human resource security solutions.

Insider threats and external threats should be managed cooperatively, as part of a comprehensive security program. However, a special focus on insiders may help organizations close the gap between external and internal security preparedness and help them get closer to where they need to be.

Many organizations will benefit from implementing a simple, three-phase approach for managing insider threats. Each phase provides insight into the nature of insider threats to the organization, and should be conducted on a continual basis.

The three phases of the insider threat management process are:

1. Assessment

In the Assessment phase, organizations seek to understand their insider threats and exposures. Organizations should make a concerted effort to audit insider activity through a number of assessment methods, including a technical exposure assessment, personnel interviews, and policy reviews. Care should be taken to conduct as wide a survey as possible and to avoid ruling out areas of the business as "off limits."

Many organizations benefit from initiating their Assessment phase with an automated technical Exposure Assessment (EA) with one of the many network monitoring tools available. During an EA, a network appliance records all activity occurring on a network, outbound and inbound. Data are collected for a period of time, usually no longer than 5 business days, encrypted for safety, and subsequently analyzed to detect activity patterns and user behavior. An EA provides a snapshot view of the policy violations that may be occurring through electronic and Internet-based communications.

For example, an EA may show that sensitive corporate data is leaking out of the organization through email, instant messaging, or other Internet-based activities. Often, the results of an EA are so illuminating (and alarming) that management will take immediate remediation steps. One remediation step might be to block all instant messaging traffic or to prevent access to certain objectionable websites.

The EA results may be used to guide personnel interviews, which seek to assess "soft" activities, such as employees taking laptop computers home from the office or "piggybacking" to gain physical access to corporate buildings and facilities. Often it is easier and more cost-effective to request employees to self-disclose behavior in a consequence-free or anonymous setting than it is to attempt to discover threatening or risky behavior through investigations, security log reviews, review of archived closed circuit television footage, etc.

Finally, a thorough review of the paper policies that have been approved by an organization is critical to assessing areas of potential weakness, even if those policies have not been fully implemented or reliably enforced. Policies may include legal and regulatory mandates, employee acceptable use and conduct guidelines, and corporate governance requirements. Based on the results of the EA and personnel interviews, a gap analysis may identify areas in which policies are poorly defined or nonexistent.

At the conclusion of a formal Insider Threat Assessment, a report should be created, integrated with the general information security policy, circulated among business stakeholders, and maintained.

2. Prioritization and Review

Once the Assessment phase is completed and an Insider Threat Assessment report has been generated, the process of business review and prioritization should occur. During this phase, key members of the IT, operations, human resources, legal/compliance, security, and senior management teams should meet to review the results of the Assessment and to identify, rank, and prioritize critical areas of concern. Organizations may choose to employ a simple scoring mechanism (e.g., a criticality range from 1 to 10) or severity labels (e.g., "low risk," "medium risk," "high risk" and "critical risk") to

assist in their efforts. Traditional risk management methodologies, including business impact analysis, qualitative risk analysis, and quantitative risk analysis, should be used to further define and determine priorities.

For example, if a bank performed an insider threat assessment and determined that their employees often wrote down email account passwords, they might determine the severity as “medium risk” with a financial exposure of \$1M/year. If on the other hand they discovered employees were stealing personal information about customers to sell to identity thieves and other criminals, they might determine it to be a “critical risk” to their business with a financial exposure of \$100M/year.

After the prioritization process, a report of findings should be created, circulated among business stakeholders, and kept up-to-date.

3. Remediation

Once insider threats have been assessed, and critical risk areas have been ranked and prioritized, an organization can begin to address and remediate threats. It is important to match any proposed remediation method to the size of the threat as determined during the quantitative analysis. If an organization cannot reasonably quantify the threat, it should look to reduce or transfer the risk as much as possible, including through specialized underwriting and insurance policies.

Remediation efforts can take many forms:

- re-installation or re-configuration of existing security systems
- purchase and implementation of new security tools
- forensic investigations
- employees awareness training
- rewriting corporate policies
- contracting for specialized consulting services
- ongoing insider threat assessments

It is essential to determine the timeframe in which remediation should and can occur, how much budget funding is available, and which departments in the organization are responsible for managing and conducting remediation efforts.

Organizations should strive for accountability in their remediation efforts, whether conducted with internal resources or external contractors, consultants, and tools. If tools are purchased, they should be implemented and optimized to the greatest extent possible. If external contractors or consultants are hired, their efforts should be audited and reviewed.

The results of the remediation phase should be integrated with the assessment and prioritization reports, and a final insider threat management report should be produced.

ADMINISTRATIVE SOLUTIONS FOR INSIDER THREATS

As discussed earlier, insider threats are personnel threats first and foremost. Accordingly, they cannot be managed by technical solutions alone. A combination of technical and administrative solutions is required to adequately defend against insider threats. Administrative solutions are not necessarily new or groundbreaking ideas to combat new risks; insiders have always presented threats to organizations through both malicious behavior and unintentional mistakes. However, administrative solutions must be kept current in order to deal with new insider threats that are created as our organizations become more technologically advanced (and dependent). Administrative solutions include 1) policies & procedures, 2) Human Resources, and 3) awareness & training.

Policies and Procedures

Developing an adequate security policy is a relatively straightforward process, but it is often overlooked or not taken seriously. Perhaps because it is so straightforward, organizations tend not to put as much effort and forethought into the process.

First, there is no “one size fits all” policy. As discussed earlier, security is at odds with productivity, and finding the right balance will depend on the organization’s industry and data sensitivity. Obviously, an organization that does military research should have a policy that offers little or no flexibility. Even financial service organizations need stringent policies that ensure the protection of sensitive customer information — security is often seen as a

competitive advantage in this industry. An architectural firm, on the other hand, may possess sensitive customer information, but customer service may be the key competitive advantage for their industry, and a relaxed security policy may be required to allow for remote computing, unsecured email transfers, and comparatively lax facility access rules.

Once the proper policies are created and implemented, they must be kept current. Many companies have long-standing policies governing email usage, but have yet to implement policies governing instant messaging usage. Organizations fail to address new technologies that create new security risks. Data leaks and the introduction of viruses occur in the same fashion via IM as they do via email, but few companies have addressed the issue. Similarly, most organizations have a policy governing laptop usage (even the Department of Veterans Affairs had one), but few have updated policy to reflect the increased usage of removable media storage devices, such as USB thumb drives, iPods, and smartphones. Over time, failure to address new technologies and new trends inevitably leads to significant security breaches.

Human Resources

In the past, human resource departments focused primarily on employee recruiting and retention, and were mainly concerned with attracting the right skills and keeping morale high. Given today's security landscape, the role of the human resources department must evolve and grow. Recruiting and retention will always be paramount, but organizations must realize that HR is the first line of defense against malicious insiders.

HR must do a better job of screening prospective employees. This includes thorough background checks on employment, criminal, and credit history. Many of the issues highlighted in "Inside the Mind of a Malicious Insider" can be vetted with mandatory background checks. Few HR departments are capable of adequately performing this task, so a third-party service typically makes the most sense.

Organizations must begin sharing knowledge among their industry peers and even their competitors. For example, in July 2006, PepsiCo informed law enforcement officials that they had been approached

by employees from Coca-Cola Corporation seeking to sell trade secrets. While certain industries are highly competitive, all organizations would benefit from increased knowledge sharing.

All too often, employees are terminated for improper conduct, including theft, but legal punishments are not pursued because of the organization's interest in quietly putting the issue to rest. However, without a criminal record on their background, these employees often wind up at competitor organizations performing the same or similar job functions. The organization that has rid themselves of the problem employee may not care if that employee is now working at a competitor, but chances are they themselves have hired an employee who committed a similar act in the past. The financial services industry is seeking to work together to combat this issue by creating a "blacklist" of terminated employees. While a blacklist creates serious questions regarding civil liberties, the point is clear — organizations must do a better job of screening out problem employees before they are hired.

Awareness Training and Education

Few things are less interesting to employees than mandatory training. So when it comes to security training — where you are essentially asking employees to take time out of their day to perform their duties more carefully (i.e., more slowly) — organizations fight an uphill battle. Nevertheless, a security policy is worthless if it is not communicated, and employees cannot be expected to follow policies and procedures if they are not trained to do so.

Security is a dry topic to many individuals, so organizations must come up with creative ways to increase participation in training and education. Often an explanation of an organization's position within a particular industry, and the ramifications of security breaches is enough to encourage abidance to security policy. Security professionals will never be at a loss for relevant examples of security breaches.

A comparison of the organization's custodial role in data protection of customer and employee records to that of an individual's concern for their own identity protection is also a useful way to drive home the need for secure operations. Few things scare people

620 as much as identity theft, and an explanation of what activities take place at that organization that could potential lead to breaches can be very effective.

Equally interesting is an explanation of the changing technological landscape. Most people have at least a passing interest in new gadgets and software programs, so an explanation of the security risks created by new technologies is useful. However you address security education and training, remember that it must always be mandatory and repetitive. Keeping it interesting can be difficult, so consider using a third party service. But employees cannot be expected to abide by policy if they are not continually reminded of the risks and understand how to behave securely.

635 The administrative methods described above are an absolute requirement for a sound security program. However, having an adequate security policy is one thing: actually enforcing that policy is something different altogether. Again, security is often at odds with speed and productivity. Too many organizations implement policy and close the books on information security. Without proper enforcement, employees will always find a way to circumvent security policy if it means they can get a jump on rush hour traffic.

TECHNICAL SOLUTIONS FOR INSIDER THREATS

Technical solutions are required to protect the organization. In addition to the firewalls, intrusion prevention systems, and anti-virus software that protect our organizations from external threats, technology is also required to prevent both malicious and accidental insider threats. These tools include secure communications, data and activity monitoring, and endpoint security.

Secure Communications

In the past, employees' means of communicating with the outside world was limited to the phones on their desks. Today's employees now enjoy a wealth of communications options, including email, instant messaging, and peer-to-peer file sharing. From a security perspective, this means that employees have a variety of ways in which to disclose sensitive information. Whether protected health information, employee data, customer information, or intellectual

property, all organizations must protect against data breaches resulting from improperly communicated information.

Given recent improvement in the available software, all organizations should implement some form of secure messaging through encryption. In the past, encrypting email was cumbersome and frustrating for the user. Today's solutions are more user-friendly and much cheaper. The stakes are too high for most regulated organizations to avoid using this security technology.

Monitoring Data at Rest and Data in Motion

Few organizations know where their data reside or go. Servers, PCs, laptops, USB thumb drives, off-site data storage, third-party vendors, email, IM, webmail, and "sneakernet" — the modern enterprise is awash in data, both at rest and in motion. It has created an unmanageable situation for today's security officer. There are simply too many methods of transmission and too many places to store data for a single individual or team to track and monitor. But with regulations such as HIPAA, GLBA, SOX, and FISMA hanging over our heads, we are responsible for overcoming this challenge.

A few years ago this was an impossible task, but given recent technological advancements, organizations both large and small have tools at their disposal to track and monitor data and insider activity. A thorough and largely automated exposure assessment can provide insight into stored data at rest. It can give organizations the ammunition to "tighten the reins" on sensitive data policies and limit access to only those individuals who need it to perform authorized job functions.

Similarly, the speed of these monitoring tools and their capabilities to enforce policy can effectively manage data in motion. Again, tools are required to enforce policy. Email encryption will still be required to protect data that need to be transmitted. But a sophisticated monitoring tool can protect the organization from employee error, laziness, or malicious action by enforcing policy on sensitive data transmission. Any organization that is affected by stringent data privacy regulations should strongly consider the monitoring tools available today.

Endpoint Security

Laptops, thumb drives, PDAs, smartphones, iPods, digital cameras — employees enjoy a wealth of technology enabling remote connectivity with powerful processing and enormous storage capabilities. Again, this technology has increased productivity, but by extending the “mobile edge” of the organization, new security risks arise. Advances have been made in patch management and software distribution that enable organizations to maintain secure PCs and data transmission, but most organizations have failed to adequately manage these new devices.

With each passing day, more and more viruses are being written to attack the mobile edge of the organization, to include PDAs and smartphones. Increasingly, employees are using thumb drives to store and transfer data. There are legitimate business needs for all of these devices. Conversely, there are many job functions that do not require any mobile devices. Managing endpoint security to include virus protection and data privacy requires a centrally administered solution with sufficient granularity to determine exactly who is authorized to use devices, what specific devices are acceptable, and how those devices are used. When sensitive data leave the security perimeter, whether on a thumb drive or a PDA, that device must be encrypted.

OBSTACLES TO INSIDER THREAT MANAGEMENT

There are no quick fixes for managing insiders and their behavior. As a result, little attention has been paid to the development or implementation of effective security measures for employees and the workplace. Historically, there have been three major obstacles: technical complexity, high costs, and the lack of senior management support (“buy-in”).

Perceived Costs

High costs, or the perception of high costs, are an obstacle for many organizations when implementing effective security measures. Security is often considered to be a pure cost item that cannot positively affect the bottom line or place the organization in a

better competitive position. Interestingly, the cost of implementing effective personnel security protections pales in comparison to the financial costs and reputation losses that can result from a breach. According to a Avivah Litan of Gartner, the cost of a security breach can be as high as \$90 per compromised customer account, as compared to \$6 per customer account for data encryption, or \$16 per customer account for a combination of data encryption, host-based intrusion prevention, and strong security audits.

Many organizations fail to recognize the potential return on investment of a sound security policies and enforcement techniques and are likely to leave themselves exposed.

Technical Complexity

Insider threats do not fall neatly into predefined categories. Employee theft of tangible assets, for example, can be easily detected and prevented using common security measures such as door locks, fences, guards, and closed circuit television cameras. External threats, such as viruses and malware, can be adequately addressed by installing and properly configuring firewalls and anti-virus software. Unlawful or dangerous insider behavior, however, is difficult to detect, deter, and address.

Some organizations will choose to ignore the threats created by insiders because of the technical complexities involved in addressing those threats. Others ignore these threats because they do not want to believe that their trusted insiders, individuals who they hired and who are part of the corporate “family,” may actually have malicious intentions. From a psychological perspective, this is similar to parents installing an alarm system for the house to keep nefarious criminals out, but failing to safeguard their valuables because they cannot believe that another family member would actually steal from them. An “ignorance is bliss” attitude may prevail in organizations that do not understand and have not investigated the behavior of insiders.

Lack of Senior Management Support

In many organizations, senior management must begin by admitting security is a competitive

advantage or disadvantage for their organization, affects the bottom line, and is not simply a cost item. A single database breach incident can lead to millions of dollars in recovery costs and erode stakeholder and customer confidence. Even in light of recent, well-publicized insider security breaches, few senior managers are ready to admit that insiders need to be scrutinized as diligently as outsiders. As with any business project, it is dead in the water without management support. Until that support exists, the security posture of many organizations will suffer and breaches will likely occur.

CONCLUSION

There is nothing magical about managing insider threats. For the most part, they are new versions of age-old problems. But for a variety of reasons, we have focused our mental energy, and our information technology spending, on external threats. These external threats will continue to require careful attention, but a strong security posture can only be achieved by managing internal and external threats in conjunction.

The process begins with the recognition that insider threats exist and that they are significant. Next, senior management must decide that they really want to protect themselves against insider threats. Security requires time and money, and any

security program will fail without management support.

Once that support exists, then the detailed process of assessment, prioritization, and remediation must begin and, unfortunately, never end. Security is not a project, it is a corporate function that continues to improve and evolve over time. Thankfully the technology exists to combat insider threats, and its growing popularity as an area of security focus and expertise means that insider threat management will become more sophisticated and economical over time.

Regardless, organizations need to do a better job in combating insider threats. An organization's security policies have a direct impact on the stakeholders who invest their time and money, and the individuals who entrust them with their most sensitive data. Insider threat management is an obligation that can no longer be ignored.

BIOGRAPHY

infoLock Technologies is an insider threat management consulting and solution provider founded in 2005 and headquartered in Arlington, VA. infoLock Technologies provides comprehensive insider threat management services, including insider activity assessment, monitoring, secure communications, and compliance management. infoLock Technologies can be found online at www.infolocktech.com.

