SpectorSoft 2014 Insider Threat Survey

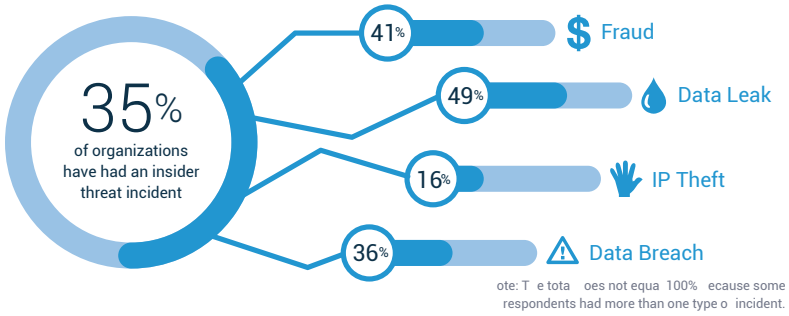
An overview of the insider threat landscape and key strategies for mitigating the threat challenge

Executive Summary

SpectorSoft recently surveyed 355 IT professionals, asking about their experience detecting and preventing insider threats, to explore how organizations are addressing this critical issue and how effective their approaches have been. Approximately 35 percent of respondents reported they had experienced an insider attack, but the situation is probably worse than they think. With an estimated 75 percent of all insider crimes going unnoticed, it seems likely that all organizations have experienced an insider crime, whether or not they know it.

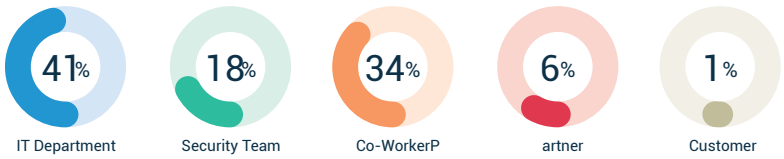
Even more sobering, the survey results suggest that the situation is unlikely to improve soon: 61 percent said they couldn't deter such attacks and 59 percent were unable even to detect one, leaving them still vulnerable to fraud, data breaches, and IP theft.

Most organizations have perimeter defenses, but as many have learned the hard way, it's also critical—and in many ways more difficult—to defend against threats inside the perimeter. Insider threats come from employees or vendors who have been authorized to access IT resources but use them in unauthorized ways. This unauthorized use can result in fraud, IP theft, data leaks, noncompliance with company standards or government regulations, inappropriate behavior, or productivity loss. The insiders may be compromising systems inadvertently—which typically has less severe consequences—or with mischievous or malicious intent, which can cause serious problems for organizations.



ote: T e tota oes not equa 100% ecause some respondents had more than one type o incident.

Insider Threat Occurrences By Department



Most of us immediately think of banking, financial services, government, healthcare, or manufacturing as being the industries most at risk from an insider attack, but other industries are also affected. In real estate, 37 percent of data attacks are from insiders,

[1]Verizon 2014 Data Breach Investigations Report

in the public sector 24 percent, in administrative organizations 27 percent, and in mining 25 percent. The inescapable conclusion is that every industry is vulnerable to some type of insider misuse, errors, or malicious attacks that can impact business operations and profitability, expose data, and deliver valuable corporate IP into the hands of competitors.

The nature of insider threats—authorized persons misusing their authorization—makes it harder to detect such attacks and protect against them. While the percentage of insider threats—approximately 30 percent of all cyber attacks—has stayed broadly consistent since 2004[2], the total number of such attacks has increased dramatically, resulting in $2.9 trillion in employee fraud losses globally per year. In the U.S. alone, the most recent year on record, organizations suffered $40 billion in losses due to employee theft and fraud—but chances are that even more fraud went undetected.

Of course, the vast majority of employees are trustworthy. Evidence suggests that just 10 percent of employees account for 95 percent of incidents. But it's hard to know who these employees are and how to prevent their attacks, especially because, according to the 2014 Verizon Data Breach Investigations Report, "most insider misuse occurs within the boundaries of trust necessary to perform normal duties." [3]

SpectorSoft sponsored this research to better understand organizations' experiences with insider threats and the challenges they face in addressing them. Through this research and related findings, SpectorSoft aims to provide organizations specific guidance on how to deter, detect, and detail insider threats, so they can protect themselves better against these damaging attacks from within.

Methodology

The results of this survey were gathered from IT security professionals within organizations conducting business in the U.S., Latin America, and Europe. The organizations ranged in size from SMBs to enterprises, and respondents' job titles ranged from general IT to security-specific roles.

Deter, Detect, and Detail: The Three Ds of Incident Response

Deter

Deterrence is the first line of defense against insider threat behavior. Deterrence means discouraging people from abusing their access privileges, typically by instilling fear of the consequences. Organizations seeking to improve their ability to deter an insider attack should consider this important finding from The Sentencing Project: "Research indicates that increases in the certainty of punishment, as opposed to the severity, are more likely to produce deterrent benefits." [4]

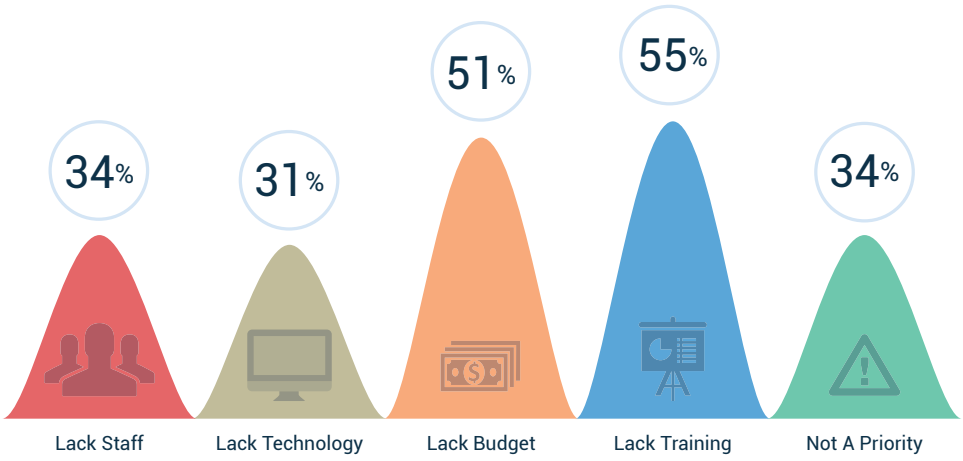
This suggests that an organization's best defense is to make sure employees and other authorized users are trained in acceptable use and informed that their computer and network activity is being monitored. Just as drivers slow down when they see a police car parked on the highway, a reminder that employees are being monitored is often enough to ensure they follow the rules that have been spelled out.

---

[2]Source: 2013 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University, and Price Waterhouse Cooper, June 2013.
[3]Verizon 2014 Data Breach Investigations Report
[4]Valerie Wright, Ph.D., Research Analyst

But while 41 percent of organizations reported that deterrence was their top priority, 61 percent admitted they didn't have the ability to deter an insider threat. The first step in deterrence is for an organization to implement an Acceptable Use Policy (AUP). An AUP serves multiple purposes. It spells out policies clearly, so employees know what is acceptable or not. And it also puts them on notice that the organization has the right to monitor activity on company-provided devices and on the company network.

Organizations should make sure all employees receive a copy of an AUP and acknowledge receiving it, either in writing during their onboarding, or better yet, every time they log on using a click-through.



Disclosure about monitoring is a best practice, whether local law requires it or not. The disclosure can be as high level as, "The company has the right to monitor all activity and communications that take place on company-owned computers, devices, and networks" or as detailed as the organization chooses to make it.

Detection

Nearly half (49 percent) of respondents said that their prevention efforts focused on detecting insider threat behavior, but despite that focus, 59 percent admitted they couldn't detect an insider threat. Though 42 percent said that detection was harder to implement than deterrence or detailing, in many ways, it's the most straightforward of the three, because it's more about technology than psychology.

Security software can monitor systems and users, comparing their actions against baseline activities and issuing timely alerts about activity, keyword use, and changes in linguistic patterns. Such software should run complex analytic and predictive algorithms in the background, while presenting intuitive dashboards that report on the results of this analytic activity in a way that makes it easy for administrators to understand and evaluate potential threats and intervene to prevent insider attacks from occurring.

Ideally, the software will also offer a range of choices in the type of monitoring an organization can implement. Active monitoring—sometimes referred to as employee surveillance—records employee digital activity and makes the collected data available for review, reporting, and retention. If there's any reason to suspect an active insider threat,

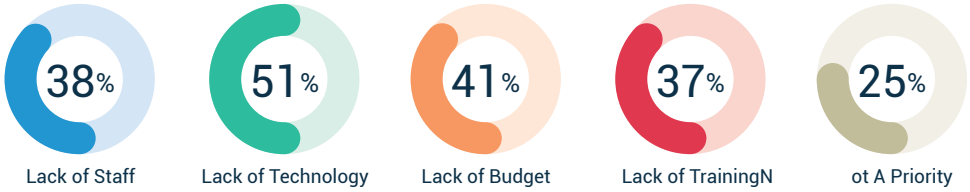
this is the approach to take. Even if they're not under immediate threat, many organizations will broadly deploy an active monitoring solution to receive the maximum benefits from their employee monitoring strategy.

Organizations that assess their risk as low might prefer to implement passive monitoring, which records employee activity and generates alerts from events detected in the employee activity logs. This does not make the collected data available for review, reporting, or retention unless there is cause to do so. Look for a solution that's configurable to allow focusing on an activity of interest. For example, phrases like "it's off the books" or "it's a gray area" that are used in communications by accounting staff may provide cause for investigating possible employee fraud.

A mix of passive and active monitoring makes sense for many organizations, as it combines broad deployment of the passive capability with targeted use of the active monitoring capability as needed.

Detail

Only 10 percent of survey respondents said that getting details on insider threat behaviors was their priority. Organizations clearly have not invested in this: 75 percent of respondents do not have the ability to detail the human behavioral activities of an insider threat.



While gathering details on an attack can't reverse the sequence of events and prevent the attack from having happened, it can still be extremely useful in mitigating the impact of an attack. By gathering detail on exactly what happened and to what extent, who was involved, and maybe even what the person's motivations were, an organization gains the data it needs to ensure that it has fully addressed possible consequences of the attack, which is important for damage limitation.

Plus, if an organization decides it must terminate insiders who seem responsible for an attack, detailed information protects the organization from an expensive wrongful termination suit, which can cost $250,000 if the organization can't substantiate its reasons for terminating an employee. With clear proof, the organization can win a summary judgment and save approximately $100,000 in legal fees. It might even deter insiders from suing at all if they believe the organization has extensive proof of wrongdoing.

Steps to take to protect your organization from insider threats

Based on what our recent survey has revealed about the threat landscape, and drawing on our own expertise in this industry, we've distilled three steps you can take right now to help defend your organization against insider threats:

1. Deterrence: Draft and implement an AUP. To get you started, here's a sample that many of our customers have used. [PDF DOWNLOAD]

2. Detection: Start talking to security experts to come up with the list of monitoring types that best fit your organization's needs. Choose from active, passive, and hybrid approaches. We recommend that you implement solutions that you can customize and extend to meet growing and changing needs, as insider threats can arise suddenly.

3. Detail: Several products on the market provide the capability to investigate details of an attack. Make sure you choose a product that can help you both limit the potential reach of damage already caused and remove the source of the threat.

How SpectorSoft can help

SpectorSoft helps organizations detect and detail insider threats by providing company-wide employee monitoring and surveillance software. The SpectorSoft suite of employee monitoring solutions enables customers to record, review, report, and retain employee activity on corporate-owned computers and networks to gain incident insight into exactly what happened, the extent of the incident, who was involved, and even why the incident happened. Its IT admin solutions allow customers to securely monitor, manage, log, and respond to critical server and desktop issues for maximum network security, integrity, uptime, and efficiency. By monitoring computer and network activity down to the keystrokes, organization's can see what employees are chatting about, what they're looking for, what they're transferring, and where they're transferring it.

See the full Infographic here »

About SpectorSoft

SpectorSoft is the leader in employee monitoring and analysis software. We've helped more than 36,000 businesses, government organizations, schools, and law enforcement agencies improve how they address security and achieve compliance across communication and computing OSes and devices. Our solutions review security risk, audit compliance mandates, protect assets and reputation, ensure adherence to Acceptable Use Policies, and optimize productivity and efficiency. For more information, visit www.spectorsoft.com.

Corporate Offices

SpectorSoft Corporation
1555 Indian River Drive, B-210
Vero Beach, FL 32960 1.888.598.2788
Toll Free Phone/Support 24/7
1.772.770.5670

West Palm Beach
1555 Palm Beach Lakes Blvd. STE 1500
West Palm Beach, FL 33401

International

United Kingdom
C2, Dukes Street
Woking
Surrey, GU21 5BH
+44 1483 397744