The Insider Threat

A layered approach can help mitigate the risks

By Marleah Blades

Each new study that is released further confirms that the malicious insider continues to pose a major threat to organizations in both the public and the private sectors.

While many of us tend to reflexively think of this insider as a disgruntled IT worker who knows how to access and change system data, the reality is that the insider can act in a variety of ways by a variety of methods to harm the organization, and he or she could be anyone. It is true that cyber attacks are a popular way for insiders to commit crimes, simply because so much business in the public and private sectors is done electronically, and because even non-technical employees — particularly in the younger generations — are more technologically savvy than they have been in the past. But focusing protection efforts on cyber controls alone is a mistake.

The threat is the individual, not the method of attack. By developing mitigation plans that include cultural shifts, training, process and policy measures rather than targeted technology alone, security professionals will have the best chance of saving their organizations from the cost and reputational damage that result from insider incidents.

The Complexities of Insider Risk

Recent reports including the Verizon/U.S. Secret Service 2010 Data Breach Report and the 2010 Cybersecurity (e-crime) Watch Survey (conducted by CSO, the U.S. Secret Service, CERT and Deloitte's Center for Security & Privacy Solutions) agree that outsiders still perpetrate the most cyber attacks and data breaches. However, the e-crime Survey and Ponemon Institute's Cost of Cyber Crime Study 2010 find that insider incidents are often more costly than external breaches. This is likely because malicious insiders are more likely than hackers or even organized groups to know what information to target and how it can be obtained.

This causes a priority problem within many organizations, says Dr. Mike Gelles, a Director with Deloitte Consulting LLP. "Many companies and public organizations think of the insider threat as a very high-impact, very low-frequency issue. While they never want it to

happen on their watch, the likelihood of it happening is not going to be that high. So managing this threat doesn't always become a high priority, which is fascinating, because the impact is so tremendous in the marketplace and the public sector."

In other cases, security professionals and business leaders may recognize the importance of protecting against the threat but feel somewhat powerless to do so. The insider threat poses a difficult challenge for a number of reasons. Among them:

- Insiders do not have to infiltrate perimeter defenses on the network or in the facility.
- They tend to plan their actions in advance and carefully cover their tracks.
- They often use appropriate and approved access to systems and areas to commit their crimes.
- They often have no criminal background.
- They may have a variety of targets within the organization and they may act based on a wide range of motivations.

Who Is the Insider Threat?

Malicious insiders may use a variety of methods to cause damage — network or manual sabotage, espionage, fraud, embezzlement, misuse of information or theft of intellectual property carried out by electronic means or on paper. They may act alone or with the support of an outside party such as an organized cyber crime group or a state-sponsored entity. The malicious insider can come from any function in the organization, and from any level — from third-party contractor to staff to executive. Some of them join specific companies with the intent to harm, while others — some studies say most — begin to contemplate such actions after experiencing a catalyst during their employment. They may want to hurt the company for revenge, or as a strategy for advancement, or they may simply be looking for a way to skim off some cash. Because these possibilities are so varied, it is nearly impossible to use method, skill set, function, job title or even motivation to effectively screen for risk potential.

Deloitte's Federal Government Services study, "Building a Secure Workforce: Guard Against Insider Threat," co-authored by Gelles and David Brant, attempts to recognize commonalities among malicious insiders. The study notes that the insider threat tends to consciously pursue his or her plan against the organization for an extended period of time, and that the intent to harm is often the end-result of problems in the person's life, such as family disputes, emotional instability, financial trouble, health problems or other stressors. It also identifies several traits that have been associated with employees who are potential security risks, including self-centeredness, feeling neglected, a sense of entitlement, passive aggressive behavior and intolerance of criticism.

"If you can capture all the data surrounding the behavior in the memory of the endpoint without them knowing you're doing it, it's very powerful forensic tool for finding malicious behavior," William Crowell says.

Park Dietz, M.D., Ph.D., forensic psychiatrist and founder of Threat Assessment Group, adds to the Deloitte findings a trait that is commonly seen both in malicious insiders and in perpetrators of workplace violence. "Bonding to the organization is impaired in both groups," he says. "Sometimes because they've been alienated by not advancing as quickly as they had hoped or by being given tasks they don't like. They may feel picked on and marginalized in the workplace."

However, Dietz cautions that security professionals must take special care when considering character traits as potential indicators of risk. "Most people with narcissistic traits are not going to commit serious misconduct in the workplace," he says. "It's a little dangerous to begin to generalize about personality types.

"It's sensible to [screen for risk indicators] in a way that's going to maximize the hit rate — it's not really sensible to do it randomly," Dietz continues.

But if an organization chooses to take character traits into account to improve their chances of identifying a potential insider risk, the security leader must be careful not to place undue burden on the false positives, or those individuals who may have the traits but cannot be shown on investigation to be a threat. "What one does with the information that someone has these traits should not be harmful to that individual," Dietz warns.

So who is the malicious insider? Clearly there are more variances than commonalities between insider threats, and the commonalities that do exist tend to be intensely personal and thus perhaps difficult to uncover or ascertain.

Because the threat is multi-faceted, guarding against it may be most effectively accomplished through a layered approach incorporating process and policy, technology and cultural change.

Know Your Assets

Before we continue, it is worthwhile to note the importance of knowing exactly what needs to be protected. Mitigation tactics will have limited efficacy if they are not based on a clear understanding of the organization's valuable assets and information. Security and risk professionals must clearly identify intellectual property, proprietary data, and assets and information at risk before embarking on a program to protect them.

"Everyone who went to high school is familiar with how popular kids target some unpopular kids...This happens in workplaces universally unless management becomes aware of the need to prevent it," Park Dietz says.

Stop Them at the Gate

The first layer of protection involves stopping the potential insider threat from becoming a part of the organization in the first place. "We don't know our workforce. Who are we hiring?" asks David Brant, Director with Deloitte Consulting.

What's more, adds Richard Lefler, former CSO of American Express and emeritus faculty member of the Security Executive Council, organizations do not know the workforces of the companies they allow inside their walls and networks. "Outsourcing has given other companies' employees access to your facilities, and that makes them an insider threat as well," Lefler says. "Lots of companies outsource things like mailroom functions, equipment maintenance, IT and telecommunications. Nearly all companies outsource one of these things. Outside company employees get approval to enter facilities, often with few limitations. If the partner has not done a good job of hiring, the threat is yours."

Mandating background checks that are stringent enough to match the value of the organization's assets is a basic measure here. Deloitte's "Building a Secure Workforce" study recommends that companies use the interview and hiring process to weed out those traits they have identified as potential risk indicators. That is, companies should seek to hire individuals who can show they are team-oriented, who respond to criticism well, and who can deal well with conflict. Dietz notes, however, that over-reliance on this approach would exclude many of the best scientists, technical innovators and sales people.

Another crucial step is developing contractual language to require due diligence of contractors, Lefler says. "When the company enters into a service agreement, they need to make sure that vendors and suppliers will maintain audit systems and controls over their employees to the extent you do over yours. Include liability language in all contracts for losses due to the actions of outsiders who violate trusts," he says.

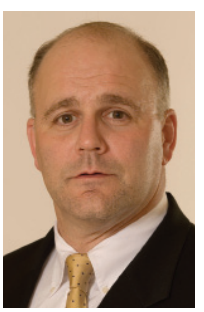
Of course, as noted previously, insider threats often come to their organizations without criminal backgrounds, so background checking will only go so far to mitigate the threat. And it may be difficult to audit a contractor's diligence in hiring for certain personality traits. That is why the next layer of measures focuses on stopping existing employees from becoming a threat to the organization.

Stop Marginalization by Fostering a Team Culture

One of reasons insiders strike out against their companies is because they have been marginalized by their peers and sometimes even their supervisors.

"Everyone who went to a public high school in America is familiar with how popular kids target some unpopular kids, often the ones who are thought of as geeky," Dietz says. "They tease them, call them names, make then the butt of jokes, don't invite them to parties and then make a point of talking about how great the party was in front of them, leading to tremendous resentment and feelings of exclusion. This happens in workplaces universally unless management becomes aware of the need to prevent it."

"Many companies and public organizations think of the insider threat as a very high-impact, very low-frequency issue...So managing this threat doesn't always become a high priority," Deloitte's Mike Gelles says.



A person's differences — ethnicity, accent, financial situation or poor social skills, for example — can be targeted by their colleagues, leading to alienation and thoughts of revenge on the individual tormentors and the organization that fails to protect them. According to Dietz, once a marginalized employee has become the saboteur or thief, management focuses only on terminating that bad actor, not on fixing the environment that helped shape him or her.

"I think the issue is for supervisors to learn about this phenomenon and not sanction or enable it," he says. "They shouldn't look the other way or participate in it, because that's what sustains this behavior. If the supervisor points out that this isn't appropriate team behavior, it can all be short-circuited. Instead, what commonly happens is the supervisor has risen from the ranks as one of the popular people and so participates in the joking or treats the individual unfairly. Part of being a leader at that level means making sure that everyone is treated fairly and no one is being singled out."

"The awareness program should make the employee comfortable with reporting and confident that the company will act appropriately in protecting employees and shareholders," Richard Lefler says.

Awareness and Reporting

Deloitte's "Building a Secure Workforce" study emphasizes the importance of training the workforce to behave as a threat monitor and maintaining a system that encourages them to report suspicious behavior. "[Malicious insider activity] is often not done in great secrecy," Lefler says. "People around them may be aware of what they are doing, but since there is not corporate sensitivity to it, employees don't always feel obligated to report what they know. That's why awareness programs are important, as are hotlines, and supervisor reporting procedures.

"The awareness program should make the employee comfortable with reporting and confident that the company will act appropriately in protecting employees and shareholders," Lefler continues. "It should be a team effort by HR, legal, security, compliance and the other business leaders. The message needs to be that it's not just about helping the company, it's about helping the employees."

Deloitte's Gelles agrees, noting that a generic awareness program conducted annually or at hiring will be far less effective than a regularly reinforced program that could amount to cultural change. "I think that's where the challenge is for companies today," he says. "They have to use not just the managers but employees to be able to be sensitized to the specific things they need to pay attention to in the specific components across the enterprise where they work." (See sidebar below.)

Brant notes that this effort is further complicated by the virtual nature of the workplace today. "Ten years ago, everything was face-to-face. Now, nearly all our communication is cyber. We have lost that element of personal interaction that allows us to see a potential problem or to deal with it. It's difficult to identify patterns of risk and to initiate follow-up when there's no personal interaction," he says.

Gelles and Brant encourage security leaders to work closely with employee assistance programs and Human Resources, both of which have unique insight into the lives of employees going through personal struggles that might spark a desire to harm the company.

Halt the Damage in Progress

If no other methods stop the insider's malicious intent, a layer of technology solutions can assist the organization in catching him or her in the act.

William Crowell, a member of the Security Executive Council Board of Advisors, recommends security incident and event monitoring (SIEM) tools, offered by companies like ArcSight and RSA. Crowell, who is also a Director of ArcSight, recently acquired by HP, further recommends tools that enable you to

Develop the Workforce as a Security Sensor and Collector

Steps to consider

- Assess the degree of vulnerability to exploitation across the employee network, including those vulnerable to exploitation and unwitting disclosures in support of their work because of a need for validation or support of a dual loyalty.
- Develop workforce standards to mitigate risk, including hiring practices, security requirements, management practices for problem employees, disciplinary procedures, resources provided to employees in crisis, and crisis management practices.
- Develop a curriculum that includes observation skills, targeted behaviors, reporting protocols, and quality assurance mechanisms (e.g., techniques to minimize false positives).
- Develop a set of specific targeted behaviors that are consistent with current preoperational tactics (e.g., patterns discerned from the case studies database, individuals who demonstrate undue interest in specific areas and functions, unusual patterns of activity such as employees being in places that are not relevant to their tasks).
- Develop training for reporting suspicious and aberrant behavior consistent with a process designed to capture data collected and reported by the workforce.
- Develop baseline awareness training as part of the on-boarding process for all employees working in the transportation system.
- Develop a generalized training for employees in noncritical vantage points, and targeted and specific training for employees in critical vantage points.
- Develop a continuing education program for all employees to update their initial training and reinforce awareness and vigilance practices as the adversary evolves.
- Develop a security plan that includes roaming interviews of the workforce in real time.
- Develop a test mechanism to ensure quality assurance and determine where additional training should be conducted.

From Deloitte Federal Government Services, "Building a Secure Workforce: Guard Against Insider Threat." Full report available from Deloitte at http://www.deloitte.com/view/en_US/us/industries/US-federal-government/764ef33b4010e110VgnVCM100000ba42f00aRCRD.htm. A related paper on maintaining the cyber secure workforce is available at http://www.deloitte.com/view/en_US/us/Services/consulting/human-capital/5deaff730dd5b210VgnVCM2000001b56f00aRCRD.htm.

track the behavior of people regardless of their credentials across applications and databases.

"Those are very powerful tools because if you have suspicions about an insider you can essentially monitor all their behaviors and activities inside your network," Crowell says. "Also important are forensic tools that allow you to capture things in memory of endpoints or workstations. If you can capture all the data surrounding the behavior in the memory of the endpoint without them knowing you're doing it, it's very powerful forensic tool for finding malicious behavior. Several companies also make ESM tools and audit and logging tools that are in appliances," Crowell continues, "which can be deployed in small to mid-size companies to pretty good effect."

It is also important to maintain robust access controls and access tracking within physical facilities to ensure employees are not attempting to access areas in which they do not belong. Lefler further emphasizes audit control over inventory, if shrinkage could be a factor: "If a company purchases 5,000 new computers and hires a company to install them, for instance, then you can control some risk by doing inventory control," he says. "Release only the number of computers that can be installed day-by-day. Maintain audit control over inventory so that shrinkage is detectable. Ask the installer to prove that computers that were provided were truly installed."

"Ten years ago, everything was face-to-face. Now, nearly all communication is cyber. We have lost that element of interaction that allows us to see a potential problem or to deal with it." Deloitte's David Brant says.

The location and value of the organization's assets at risk will determine the best technologies and policies for detecting potential insider misconduct. But all organizations can benefit from a layered strategy that has the best potential for stopping potentially malicious insiders both before and during an event. ▮

Marleah Blades is senior editor for the Security Executive Council (www.securityexecutivecouncil.com/?sourceCode=std), which provides strategy, insight and resources to risk mitigation decision makers. The Council incorporates input from industry segments into proven practices to provide options that solve pressing issues. With a faculty of more than 100 successful experienced security executives, we work one-on-one with Tier 1 Security Leaders™ to help them reduce risk and add to corporate profitability. To learn about becoming involved, e-mail contact@secleader.com.