5 Tips for Stopping Insider Threats

[fa icon="calendar"] May 13, 2016 8:35:21 AM / by Michael Stone

Employers bring on people who have the skills, who have the certifications, who often have longevity in the field, and who they think they can trust. But in an increasingly complex, globalized, ruthless world, the trust portion is becoming harder and harder to find — and when a breach happens, the company has to scramble to reassemble the wreckage.

These internal misuses of trust are commonly referred to as "insider threats." The term is defined by Carnegie Mellon University's Software Engineering Institute, a lead researcher on the topic, as an employee, former employee, contractor or business partner who has authorized accesses and "intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity or availability of the organization's information or information systems."

Though insider threats are often unknown to the public, especially those that happen within private companies, some do catch the spotlight because of factors including notifications to affected customers and governmental entities having the data handed off to the media.

These could range from simple modifications or thefts of information to elaborate operations of sabotage. A specific tactic that has been increasing in recent years, the FBI says, is employees stealing insider information from their current employer to sell them or for use at their next job.

Filter by Topic

Perhaps the two most well-known cases in recent memory are the government leaks from Army Pfc. Bradley Manning and NSA contractor Edward Snowden. Others, as noted by the FBI, include:

- ✔ Research scientist Wen Chyu Liu was convicted in 2011 of taking trade secrets from his employer to sell them in China. Among his activities: paying former and current employees of the company for information, bribing one of them with $50,000 for specific information, and traveling throughout China to market the information.
- ✔ Computer programmer Sergey Aleynikov was found guilty in 2010 of theft of trade secrets after he attempted to take 32 megabytes of his Wall Street company's computer codes in his final days at the job.
- ✔ Chinese spy Greg Chung was sentenced to jail in 2010 after taking thousands of documents about the space shuttle and other U.S. flight programs from 1979 to 2006 and giving them to China.

Having such an infiltrator isn't lightning-strike odds, according to a 2011 survey by the institute, the U.S. Secret Service and others. Of the surveyed organizations that knew the identity of the threat, 21 percent said the act was done by someone on the inside.

When establishing preventative measures, it's essentially a necessity for organizations to be exceedingly cautious and go beyond basic levels of security because of the assumed level of sophistication and determination by the attacker, as well as the possibility that she or he is being supported by an external advanced persistent threat.

Common recommendations from the institute, the FBI and other experts include:

1. Being overly strict on enforcing the separation of duties in privileges, meaning a user has access only to the extreme minimum she or he needs.
2. Having standard procedures or software, such as an intrusion detection and prevention system, in place to monitor all users' movements.
3. Establishing a standard disciplinary procedure — whether it be a warning, strike or instant-termination system — for if and when an employee ventures outside the scope of her or his accesses. Also, this procedure should be a living document to account for any new situations, and employees should be notified of such additions.
4. Providing an outlet — perhaps even one that grants anonymity — for employees to report suspicions.
5. Avoiding instantly alerting the person under suspicion. This would give experts time to step in to analyze any damage and possibly mitigate it before the alleged attacker has a chance to make matters worse, untraceable or too far gone to be helped.

For those wanting formal training in combatting insider threats, the institute offers certification

courses throughout the year.

Read about advanced technology that can better protect your organization's data

Download Now

Written by Michael Stone

Michael Stone is a writer and photographer based in Gainesville, Florida, who has had his work published in several newspapers, magazines, and websites. He writes about a variety of topics, including technology and its impact on healthcare and education. He holds degrees in journalism and communications from the University of Florida and Middle Tennessee State University. You can read more about him on his website, www.MichaelStoneOnline.com.