Your cubemate is probably the trustworthy confidante you always assumed her to be, or she might be someone who is very good at hiding her intent to take valuable information off the premises for her own use. Or maybe she is a good person—just a misguided one who doesn’t understand that her actions constitute an insider threat.

There are many faces to insider threats, and they are often very difficult to identify. Here are some of the most important:

• The disgruntled employee: This employee has an axe to grind, and does it by creating malware or leaking valuable information online or to others. Some also are motivated by wanting revenge for some action they perceive as negative toward them.

• The maverick: These people just want to get their jobs done, and they will circumvent policies to do it. Those policies are designed to mitigate risk, and by avoiding them, these employees are inadvertently exposing the organization and its data. Some mavericks also want to challenge the system and take it too far.

• The innocent: These employees have no idea that their actions are putting the organization and data in danger. It can happen by copying files that shouldn’t be copied, emailing information that shouldn’t be emailed, using a mobile device for work-related tasks without the right controls, or taking work home that should stay on the premises.

• The thief: Whether it’s a slow and steady scam or a fast data grab, these employees or contractors are on a mission to steal valuable data. The slow and steady scam is more prevalent; according to research by Carnegie Mellon University’s Software Engineering Institute, employees typically work at a job for more than five years before they start committing fraud. Even more surprising, it takes employers almost three years to find out what those employees are up to.

### INSIDER THREATS BY THE NUMBERS

14
The percentage of total incidents attributable to insider threats
Source: Verizon’s 2013 Data Breach Investigations Report

28
The percentage of insider threats carried out via portable equipment
Source: CERT Insider Threat Team

87
The average number of days for an organization to discover a case of insider fraud
Source: Ponemon Institute “2013 Risk of Insider Fraud”

1.5 million
The average amount of damage caused, in dollars, by managers found guilty of insider fraud
Source: Ponemon Institute “2013 Risk of Insider Fraud”

17
The percentage of insider threats caused by malware or spyware
Source: CERT Insider Threat Team

49
The percentage of unintentional insider threats caused by accidental disclosure of personal information via the Internet, mishandled or sent to the wrong party
Source: CERT Insider Threat Team

188
The cost, in dollars, of one lost or stolen records
Source: Ponemon Institute “2013 Risk of Insider Fraud”
Attacking Insider Threats with Technology

Cyberthreats of all types are more difficult to detect than ever before, thanks to more efficient and intelligent malicious software, increased use of mobile devices, the volume of network activity and the explosion of cloud computing. At the same time, cybercriminals are becoming more clever, using everything from remote access software, e-mail and instant messaging to removable devices and peer-to-peer networks.

The key is attacking from as many points as possible. That means incorporating several approaches and technologies to ensure that nothing falls through the cracks. In addition to the basics—firewalls, antivirus software, intrusion detection and prevention systems, messaging security, VPNs and secure Web gateways—consider these defenses:

Network-based database activity monitoring: This technology monitors networks to show who is viewing data, how it is being viewed, and when it was viewed. It does this by capturing and logging packets that contain Structured Query Language in real time. When one is found, the technology analyzes the SQL logic to ensure that it is authentic.

Network traffic flow analysis: NetFlow takes Simple Network Monitoring Protocol (SNMP) a few steps further to continuously evaluate who is sending network traffic, what type of traffic is traversing the network, and where it’s going, down to specific IT addresses and ports. This is one of the best ways to catch anomalies in network traffic flow in real time.

SIEM: Security information and event management helps pinpoint potential threats by using a multipronged approach. It gathers log data from an organization’s network devices and security software and combines it with analytics to find suspicious activity, vulnerabilities and configuration weaknesses.

Breach detection system: Detecting malware, especially targeted, persistent attacks, has become more difficult as the malware becomes more complex and the perpetrators more knowledgeable. Breach detection systems go a step beyond many intrusion detection and intrusion prevention tools to find both attempted and actual breaches, along with unknown malware.

Threat modeling and forecasting: If you can know in advance what threats are likely to occur in your environment, and in what timeframe, you are much more likely to be able to mitigate those threats. That’s the idea behind threat modeling and forecasting. Threat modeling allows organizations to model their specific security layers and pinpoint which threats are likely to infiltrate those layers. Threat forecasting provides the data that allows organizations to understand what threats are the most critical at any given time.

Behind the Scenes: Planning Makes all the Difference

While technology is a critical force in detecting and mitigating insider threats, all of the technology in the world won't do much good without support, policies and controls to back them up. It might not be high profile, but planning behind the scenes is imperative for controlling insider threats.

• Policies: It may be hard to believe, but about one-third of organizations have no formalized insider threat response plan, according to PwC’s 2013 State of Cybercrime Survey. It is critical to create formal policies and procedures around what is acceptable behavior, access levels (from least privilege to need-to-know), monitoring during layoffs and termination of employment, and a privacy policy that details what type of information can and cannot be accessed and retained.

• Training: Periodically, employees should undergo security awareness training, which will update them on how to detect and report suspicious behavior. This should include both hands-on demonstrations, what-if scenarios and role-playing.

• Physical controls: Policies only go so far. Physical controls—everything from biometric scanners, numeric PINs, motion sensors and security cameras to security guards and alarmed gates/doors—reduces the chances that data will walk out the door.
One of your employees hasn’t taken a vacation in two years. Another recently started working at 6 a.m. and doesn’t leave until after 8 p.m. Someone else in your organization has changed his or her home address three times this year. You have a contractor whose contract ends in two weeks.

It’s not easy to discover the malicious insider. In most organizations, employees are credentialed users of an agency’s system and are assumed to be trusted. That’s because the prevalent technology used to help pinpoint security threats—intrusion detection systems, data loss prevention systems, security incident and event management tools, anti-spyware software, and data from firewalls, routers and switches—don’t provide the context required to know the difference between innocent behavior and the actions of a malicious insider.

You can systematically identify cases of insider fraud by thinking differently about your data and asking the right questions of a big data system that can collect any type of data, even from external publicly available databases. You must combine system, application and log data with data generated from security point solutions and adding contextual data locked in business systems and other third party sources. Then ask the right questions to understand who may be perpetrating fraud.

Context is key to knowing intent. An employee may do something against policy, but may not know he or she is committing an act that could be perceived as a data breach. It’s not enough to know that an employee started using printers on another floor or sent a large document to a new address. If you know the employee’s credit score dropped 200 points over two months, their home address or banking information changed multiple times in a short period, or they spent hours online researching travel in a specific country, the picture changes.

Finding the smoking gun
Three types of data are required to separate what is normal from abnormal: Statistical analysis that can highlight behavioral outliers; log data, which is the definitive record of machine-to-machine and human-to-machine interactions; and contextual data. Collecting and correlating this data allows you to understand potential motive.

Many agencies already have the technology to do this, whether they realize it or not. Employment agreements give the employer the right to review or gather credit data or data from other publicly available sources.

Splunk, a leading platform for operational intelligence already in use by hundreds of government agencies, is more than just a big data platform that gathers and analyzes a variety of machine and database data. Applying it to this use case and asking the right questions can help you guard against insider fraud.

Splunk software collects, indexes and performs statistical analysis on data sets. For example, an analyst searches for the term “fail” and Splunk returns all data with that word. The analyst then drills into specific sources for more details. He or she also inputs a query to find all failed logins across a specific set of systems from a specific department over a specific time. In one case, an organization discovered an insider threat during a preliminary proof-of-concept with Splunk Enterprise by first detecting suspicious activity around his communications and then examining his access to a code repository. He was fired.

None of this eliminates the need for monitoring changes of routine, lack of vacation time use (which can mean an employee doesn’t want to pass responsibility to another), and emotional and psychological stresses, such as marital status changes. By combining conscious awareness with sophisticated security tools and big data analytics, agencies will make more progress in detecting and mitigating insider threats.

For more information and to download Splunk Enterprise for free, visit www.splunk.com/insiderthreat