The problem with signatures is that an administrator must know about an attack in order to create a signature for it. The first time an attack occurs, it becomes successful because there is no signature. After it is successful and the administrator performs incident response and damage assessment, he or she can figure out how the attack occurred and can build an appropriate signature for the next time; however, if the next time the attacker attacks in a different manner, the signature might miss the attack again. This brings up two important points with regard to signatures. First, they will only catch known attacks; they will not catch zero-day attacks. A zero-day attack is a brand new attack that has not been publicized and is not well known. Second, signatures are rigid. If an administrator has a signature for an attack and it occurs exactly the same way each time, he or she can detect it and flag it. However, if it is morphed or changed, there is a good chance the signature will no longer be effective. The last problem with signatures is that they take a default allow stance on security. A default stance blocks what is malicious, and anything else that falls through is flagged as good. By itself, signature detection says if there is bad behavior but there is no signature match, then the behavior must be good.

**Key Findings from U.S. Secret Service and CERT Coordination Center/SEI Study on Insider Threats**

A U.S. Secret Service and CERT Coordination Center/SEI study revealed the following things concerning insider threats:

- A negative work-related event triggered most insiders’ actions.
- The most frequently reported motive was revenge.
- The majority of insiders planned their activities in advance.
- Remote access was used to carry out a majority of the attacks.
- Insiders exploited systematic vulnerabilities in applications, processes, and/or procedures, but relatively sophisticated attack tools were also employed.
- The majority of insiders compromised computer accounts, created unauthorized backdoor accounts, or used shared accounts in their attacks.
- The majority of attacks took place outside normal working hours.
- The majority of the insider attacks were only detected once there was a noticeable irregularity in the information system or a system became unavailable.
- The majority of attacks were accomplished using the company’s computer equipment.
- The insiders not only harmed individuals but also the organizations.

**Netspionage**

Netspionage is network-enabled espionage, in which an attacker uses the Internet to perform corporate espionage. Corporate espionage is an old practice, but the advent of the Internet has made it easier, faster, and much more anonymous. Netspionage enables spies to steal sensitive corporate information without physically entering the company’s premises.

**Investigating Corporate Espionage Cases**

The following are some steps an investigator should take when investigating corporate espionage cases:

1. **Check the possible points of physical intrusion**: Before starting an investigation into a corporate espionage case, an investigator should scan all possible points of physical intrusion carefully. These points may provide clues about how the information might have leaked and can also provide fingerprints if anybody passed through. This information may be helpful when presenting the case before a court of law.
2. **Check the CCTV records**: An investigator should check all CCTV records for any unusual activity. This often leads to the real culprit.
3. **Check e-mails and attachments**: An investigator should check all official e-mails and other e-mails with attachments used at the workplace. In many cases, the information is passed outside using e-mails. An investigator should thoroughly scan any suspicious e-mail and try to find out its destination.