• **Network leakage**: Most organizations set up their network to block or limit inbound and outbound connections. Even organizations that are starting to filter outbound traffic still allow certain traffic out. Two types of traffic that are always allowed out of an organization are Web and e-mail traffic.

• **Cryptography**: Cryptography is a technique to garble a message in such a way that the meaning of the message is changed. Cryptography starts with a plaintext message, which is a message in its original form. An encryption algorithm garbles a message, which creates ciphertext. A decryption algorithm can later take the ciphertext and convert it back to a plaintext message. During the encryption and decryption process, what protects the ciphertext and stops someone from inadvertently decrypting it back to the plaintext message is the key. Therefore, the secrecy of the ciphertext is based on the secrecy of the key and not the secrecy of the algorithm. Thus, to use an encryption program, a user has to generate a key. The key is often tied to a username and e-mail address. No validation is performed, so an attacker can put in bogus information that could be used later to launch a man-in-the-middle attack where the attacker can trick someone into using a false key. If someone knows the public key for a user, he or she can encrypt a message; but he or she can only decrypt the message if he or she knows the user’s private key. The public key can be distributed via a trusted channel, but a user’s private key should never be given out. If someone can get access to a user’s private key, he or she can decrypt and read all that user’s messages.

• **Steganography**: Steganography is data hiding and is meant to conceal the true meaning of a message. With steganography, a user has no idea that someone is even sending a sensitive message because he or she is sending an overt message that completely conceals and hides the original covert message. Therefore, cryptography is often referred to as secret communication and steganography is referred to as covert communication. Insiders often use steganography to transmit credentials to other organizations.

### Defense Against Corporate Spying

The following are some techniques that can secure the confidential data of a company from spies:

- **Controlled access**
  - Encrypt the most critical data.
  - Never store sensitive information on a networked computer.
  - Classify the sensitivity of the data and thus categorize personnel access rights to read/write the information.
  - Assign duties to personnel where their need-to-know controls should be defined.
  - Ensure authorization and authentication to critical data.
  - Install antivirus software and password-protect the secured system.
  - Regularly change the password of confidential files.
  - Separate duties.

- **Background investigations of personnel**
  - Verify the background of new employees.
  - Do not ignore physical security checks.
  - Monitor employee behavior.
  - Monitor systems used by employees.
  - Disable remote access.
  - Make sure that unnecessary account privileges are not allotted to normal users.
  - Disable USB drives on employees’ systems.
  - Enforce a security policy that addresses all employee concerns.

The following are the basic security measures to protect against corporate spying:

- Destroy all paper documents before trashing them. Secure all dumpsters and post “NO TRESPASSING” signs.
- Regularly conduct security awareness training programs for all employees.