Corporate espionage: Espionage means collecting information about an enemy or a competitor through spies. Corporate espionage is all about collecting information such as client lists to perpetrate frauds and scams in order to affect a rival financially. For this reason, companies focus specifically on such crimes and take special care to prevent such situations. Experts have sketched out a two-pronged strategy for overcoming this situation as follows:

- **Knowledge of employees**: Conducting background checks on new employees, and keeping a check on employees who have been assigned sensitive projects is crucial.
- **Access control**: Information about the business that is critical or important should not be stored on a computer that is connected to a network. Data that is highly critical should be encrypted.

Child pornography: Child pornography is any work that focuses on children in a sexual manner. The global community has realized that children are at risk and can suffer from negative effects because of pornographic exploitation. Rapidly expanding computer technology has given access to the production and distribution of child pornography. Not only girls and boys but also infants are becoming victims of such offensive activity. Pornographers make use of poor children, disabled minors, and sometimes neighborhood children for sexual exploitation. Children who are sexually exploited through pornography suffer from mental depression, emotional withdrawal, mood swings, fear, and anxiety.

Luring children via chat rooms: Kidnappers often use chat rooms to turn children into victims. A kidnapper tries to build a relationship with children by showing them cartoons, interesting art clips, and offering them sweets. This is known as *grooming*. With many people of different ages, including children and youth, having access to the Internet, children are easily trapped and kidnapped because of their innocence and trust.

Scams: The Internet is globally uniform and serves as the best-known market to promote businesses and services for customers around the world. Yet it is difficult to track and differentiate between legal and fake sellers on the Internet. Fake sellers cheat people by using various options available on the Internet, such as e-mail, chat rooms, and e-commerce sites.

Cyber terrorism: Cyber terrorism is committed using computer and electronic attacks. Cyber terrorists can sit on one system and carry out attacks on computers worldwide.

Creation and distribution of viruses and spam: A virus is a program that spreads from machine to machine, usually causing damage to each system. These are some forms of viruses:

- A polymorphic virus is one that produces varied but operational copies of itself.
- A stealth virus is one that, while active, hides the modifications it has made to files or boot records.
- A fast infector infects programs not just when they are run, but also when they are simply accessed.
- A slow infector will only infect files when they are created or modified.

The following are some of the reasons individuals create viruses:

- It is a way of attracting attention.
- Virus writers gain a sense of fulfillment from creating something that impacts a vast number of people.
- It is motivated by financial gain.
- Virus writers may get excited about every bit of junk e-mail they get as a result of their virus.

The following are some of the forms in which a virus can be distributed:

- **Removable disks**: This includes floppy disks, CD-ROMs, and USB drives.
- **Crack sites**: These are sites that provide information on how to crack different applications and software.
- **Unsecured sites**: These are Web sites that do not use the HTTPS protocol.
- **Flash greetings**: This is the most common way of spreading a virus. This is a Flash animation or video that hides a virus.
- **E-mail attachments**: Users should not open attachments from unknown persons or Web sites.
- **Downloading**: Users should check Web sites to make sure they are legitimate before downloading.