

• Infection of the organization's systems or network by viruses, worms, trojans, adware or spyware

**Malware**



• Impersonation of the organization through email or electronic means in an attempt to obtain confidential information

**Phishing**



• Diversion of internet traffic to an imposter site by means of DNS poisoning or browser address bar attack in an attempt to obtain confidential information.

**Pharming**



• Unsolicited or unwanted email messages

**Spam**



• Attempts to overwhelm or overload the organization's network or system resources with the intent to degrade their performance or make them unavailable

**Denial of Service**



• Unauthorised access or use of systems or the network by outsiders

**Unauthorised access by outsiders**



• Defacement, destruction or other damage to the organization's systems, network or website

**Vandalism/  
Sabotage**



• Demands for money or other concessions based on threats to use electronic means to harm the organizations network, systems or reputation.

**Extortion**



• Fraudulent electronic transections that result in financial loss or damage to the organization or its customers

**Fraudulent Transection**



• Physical loss or theft of computers, storage media, or other devices and any associated data

**Physical Loss**



• Successful access by insiders to system functions or information for which they are not authorised

**Unauthorised access by insiders**



• Violation of the organisation's policies regarding acceptable use of computing/network resources

**Insiders Misuse**

