Cyberthreat Types and Correlated Attacks  
Technological Risks  
These dangers take advantage of holes in networks, applications, or systems.  
  
Malware is malicious software that targets and damages systems.  
Attack types include malware, trojans, worms, viruses, and ransomware.  
Denial of Service (DoS): Flooding a system with traffic in order to block access by authorised users.  
Attack types include volumetric, protocol, and distributed denial of service (DDoS) attacks.  
Attacks using weaknesses in web applications are known as web application attacks.  
Attack types include session hijacking, SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).  
Misconfigured systems or services are referred to as system misconfigurations.  
Potential assaults include system malfunctions, unauthorised access, and data breaches.

Dangers of Social Engineering  
These risks use psychological tricks on people to obtain information or access without authorisation.  
  
Phishing: Tricking someone into divulging private information.  
Attack types include vishing (voice phishing), smishing (SMS phishing), and email phishing.  
Spear phishing: Phishing assaults that are specifically targeted at particular people or companies.  
Two types of attacks include clone phishing and whaleing, which targets high-level executives.  
Physically trailing authorised individuals into restricted zones is known as tailgating.  
Attack types: Shoulder surfing (seeing what the user does).

Dangers to the Body  
These dangers entail actual physical harm to infrastructure or hardware.  
  
Natural disasters include hurricanes, floods, fires, and earthquakes.  
Possible effects include business interruption, equipment damage, and data loss.  
Physically removing hardware or data is called theft.  
Types of attacks: identity theft and burglary.  
Vandalism is the deliberate destruction of property.  
Possible effects include data loss and system outages.