12 Enterprise Mobile Threats

1 Privacy-intrusive applications
Unauthorized access to sensitive information via a malicious or privacy-intrusive application

2 Account credential theft through phishing
Theft of credentials through a short message service (SMS) or email phishing campaign

3 Malicious applications
Unauthorized applications installed via URLs in SMS or email messages

4 Outdated phones
Confidentiality and integrity loss due to exploitation of known vulnerability in the operating system or firmware

5 Cameras and microphones remote access
Cameras, microphones, or other device sensors are misused without the device owner's knowledge

6 Sensitive data transmissions
Data in transit is eavesdropped on

7 Brute-force attacks to unlock a phone
Compromise of device integrity via brute-forced device unlock code

8 Weak password practices protection
Unauthorized access to remote services via authentication or credential storage vulnerabilities

9 Unmanaged device protection
Unauthorized access of enterprise resources from an unmanaged and potentially compromised device

10 Lost or stolen data protection
Loss of organizational data due to a lost or stolen device

11 Protecting data from being inadvertently backed up to a cloud service
Loss of confidentiality of organizational data due to its unauthorized storage in non-organizationally managed cloud services

12 Personal identification number (PIN) or password-sharing protection
Unauthorized access to work applications via bypassed lock screen