Mobile Computing Device Vulnerabilities, Threats and Risks

An IT auditor should understand mobile media and devices can also be used by an individual to steal data and programs for personal use or gain. Review the chart below to learn more about the vulnerabilities, threats and risk.

Vulnerability	Threat	Risk
Information travels across wireless networks that are often less secure than wired networks.	Malicious outsiders can do harm to the enterprise.	Information interception resulting in a breach of sensitive data, enterprise reputation, adherence to regulation or legal action
Mobility provides users with the opportunity to leave enterprise boundaries and thereby eliminates many security controls.	Mobile devices cross boundaries and network perimeters, carrying malware, and can bring this malware into the enterprise network.	Malware propagation, which may result in data leakage, data corruption and unavailability of necessary data
Bluetooth technology is very convenient for many users to have hands-free conversations; however, it is often left on and then is discoverable.	Hackers can discover the device and launch an attack.	Device corruption, lost data, call interception, possible exposure of sensitive information
Unencrypted information is stored on the device.	If a malicious outsider intercepts data in transit or steals a device or if the employee loses the device, the data are readable and usable.	Exposure of sensitive data, resulting in damage to the enterprise, customers or employees
Lost data may affect employee productivity.	Mobile devices may be lost or stolen due to their portability. Data on these devices are not always backed up.	Workers dependent on mobile devices unable to work in the event of broken, lost or stolen devices and data that are not backed up
The device has no authentication requirements applied.	If the device is lost or stolen, outsiders can access the device and all of its data.	Data exposure, resulting in damage to the enterprise and liability and regulation issues
The enterprise is not managing the device.	If no mobile device strategy exists, employees may choose to bring in their own unsecured devices.	Data leakage, malware propagation or unknown data loss in the case of device loss or theft.
The device allows for installation of unsigned third-party applications.	Applications may carry malware that propagates Trojans or viruses; the applications may also transform the device into a gateway for malicious outsiders to enter the enterprise network.	Malware propagation, data leakage or intrusion on enterprise network