Vulnerability	Threat	Risk
Information travels across wireless networks, which are often less secure than wired networks.	Malicious outsiders can do harm to the financial institution.	Information interception resulting in a breach of sensitive data, financial institution reputation, adherence to regulation, legal action.
Mobility provides users with the opportunity to leave financial institution boundaries and thereby eliminates many security controls.	Mobile devices cross boundaries and network perimeters, carrying malware, and can bring this malware into the financial institution 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.	In the event that a malicious outsider intercepts data in transit or steals a device, or if the staff member loses the device, the data are readable and usable.	Exposure of sensitive data, resulting in damage to the financial institution, employees, or customers.
Lost data may affect staff productivity.	Mobile devices may be lost or stolen due to their portability. Data on these devices are not always backed up.	Staff 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.	In the event that the device is lost or stolen, outsiders can access the device and all of its data.	Data exposure, resulting in damage to the financial institution and liability and regulation issues.
IT is not managing the device.	If no mobile device strategy exists, staff may choose to bring in their own, unsecured devices. While these devices may not connect to the virtual private network (VPN), they may interact with e-mail or store sensitive documents.	Data leakage, malware propagation, and 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 financial institution's network.	Malware propagation, data leakage, and intrusion on financial institution's network.

Source: ISACA – Securing mobile devices, 2010