7.11.2 BYOD Security Facts

In addition to mobile devices owned by your organization, you must also take into account personally-owned mobile devices that employees bring to work and use to complete daily work-related tasks. This practice is sometimes referred to as *bring your own device* (BYOD). Even though it entails a host of security risks, this is very common practice in the modern work environment. Security administrators need to keep the following BYOD security issues in mind:

BYOD Issue	Description	Possible Remedies
Malware Propagation	If a user's tablet or phone is infected with malware, then the infection can be spread when they connect their device to your organization's network.	Consider implementing a network access control (NAC) solution that remediates devices before allowing them to connect to your network. Alternatively, consider implementing a guest wireless network that is isolated from your organization's production network. User-owned devices can connect to this network to gain internet access, but are quarantined from the rest of your organization's production network.
Loss of Control of Sensitive Data	If a user copies sensitive data to their device, your organization could potentially lose control of that information. Even the question of who owns the data after it has been copied to the personal device becomes problematic. Consider the following scenarios: ▪ The user may not have implemented appropriate security settings on their device, allowing anyone who gains access to the device to view the sensitive data. ▪ The user may lose the device, allowing anyone who finds it to access the sensitive data. ▪ The device may become infected with malware, potentially exposing the sensitive data.	Implement an acceptable use policy that defines what kind of data is allowed on personally-owned devices and what kind of data is prohibited. Information classification labels can be useful when implementing this policy. Consider requiring personal devices to be enrolled with a mobile device management infrastructure, such as Windows Intune, to enforce mobile device security policies.
Malicious Insider Attacks	If a user is so inclined, they could use their mobile device to conduct a malicious insider attack. For example, they could: ▪ Use the built-in camera, which nearly all modern mobile devices have, to take pictures of sensitive internal information. ▪ Use the built-in microphone to record conversations. ▪ Use the built-in video function to record proprietary processes and procedures. ▪ Use the device's mobile broadband connection to transfer stolen data to parties outside the organization, bypassing the organization's network security mechanisms.	Implement an acceptable use policy that: ▪ Specifies where and when mobile devices can be possessed within the organization. For example, the possession of mobile devices may be prohibited in high-security areas. ▪ Notifies users that personally-owned devices are subject to random searches if brought on site.
Device Management	If a user brings a personally-owned device on site, the organization needs to address clearly who is responsible for managing the device. Responsibility for the following needs to be defined: ▪ Operating system updates ▪ App updates ▪ Anti-malware installation ▪ Anti-malware definition updates	Relying on the end user to implement these updates is unwise. Instead, consider implementing a network access control (NAC) solution that remediates devices before allowing them to connect to your network.
Support	If a user brings a personally-owned device on site, the organization needs to address clearly who will provide support for the device and for the apps used on the device. Will the organization's help desk provide support, or must the user depend upon support provided by the device manufacturer?	Implement an acceptable use policy that specifies: ▪ Where users can get support for personally-owned mobile devices. ▪ Which apps are allowed for use with organizational data. ▪ Where users can get support for these apps.

To better secure mobile devices used by company employees, consider the following deployment model alternatives to BYOD.

- *Corporate-owned*: A corporate-owned device strategy lets businesses more effectively monitor and control activities performed on mobile devices. One advantage of this model is that businesses can purchase devices at significant discounts. The corporate-owned model also includes the option of restricting mobile device use to the workplace only. However, employees who need access to corporate email and other data after hours may feel compelled to use their personal devices for such access.

- *Corporate-owned, personally enabled (COPE)*: The COPE model gives businesses significant control over device security while allowing employees to use the devices to access both corporate and personal data. Because the company owns the device, it can be secured more easily and wiped clean if lost or stolen. One disadvantage of this model is that employees who are not free to choose their own devices may end up bringing their own anyway.
- *Choose your own device (CYOD)*: The CYOD model provides slightly more flexibility in giving users a limited selection of devices to choose from. But since the devices are still corporate-owned, IT managers can implement more effective security measures to prevent breaches.
- *Virtual Desktop Infrastructure (VDI)*: VDI can be used with any of the above models, including BYOD, to allow mobile devices to establish a remote connection to a virtualized desktop. Using VDI provides enhanced security and better data protection because most of the data processing is provided by servers in the data center, rather than on the local device.
