Student Guide

Cybersecurity and the Use of New Personal Devices Short

Contents

Cybersecurity and the Use of New Personal Devices

Introduction

Coworker: "Hey, check out this new fitness tracker—my wife got it for me! It tracks my steps and activity and sleep. Pretty cool, huh?"

Your coworker just returned from the holidays with a new fitness band, a wearable technology trend you've started to see everywhere. As a Security Specialist for your organization, you aren't sure what to do. Are personal devices like this fitness band allowed in closed areas with classified information? Could personal devices even put national security at risk?

Welcome to the Cybersecurity and the Use of New Personal Devices short. This short will review the role that you, a Security Specialist, must play in assessing and managing the risks presented by new personal electronic devices.

Examples of New Technology

Technology changes much more quickly than policy, and new products create new challenges for security.

New Technologies include, but are not limited to: new products for data storage, communications, access control, and intrusion detection; new online technologies, such as internet-based social media; and new personal device technologies.

Personal devices include hand-held and mobile technologies, some of which have wireless capabilities, such as smartphones and tablets, smartwatches, video recording devices, and even wearable medical devices.

Some of these devices may not meet security requirements, and organizations may restrict or prohibit their use entirely, but other organizations may allow them under certain circumstances.

Consider the example presented earlier. Some agencies have authorized the use of personal fitness devices in their facilities, including SCIFs and areas with Secret open storage, provided appropriate procedures are followed.

Risks of New Technology and Mitigation Strategies

In your role as Security Specialist, remember that even when technological change outpaces policy, fundamental risk mitigation principles still apply. Determine what risks a new technology may present, and then develop strategies to mitigate those risks. These principles provide a foundation for dealing with all new capabilities, including new personal device technologies.

For example, one potential risk presented by personal devices is that they could interact with agency systems via a wireless or USB connection. This could allow the storage of data in unsecured locations or the transmission of malware.

The use of location services on personal devices may also present risks in some cases, since these devices could disclose information about the user and about activities performed in a particular location.

To address these risks, various risk mitigation strategies may be implemented. The following are just some of the potential risk mitigation strategies for both interactions with other systems and use of location services:

- Interactions with other systems:
  - Apply security controls that restrict syncing
  - Limit the use of charging or USB devices
  - Prevent remote backup services
  - Use physical shielding to prevent data exchange
- Use of Location Services
  - Disable location services
  - Prohibit the use of location services

An Example of Risk Mitigation

Consider the example of your coworker with the new personal fitness device. Although these devices may present some risk, they also provide significant benefits for users.

Consider these possible mitigation strategies:

- Devices must be:
  - Commercially available in the U.S.
  - Marketed as a fitness/sleep device
  - Designated as an FCC-Class B digital device
- Devices must NOT:
  - Have Wi-Fi or Cellular capability
  - Be capable of photo, video, or audio recording
- Users must NOT:
  - Connect devices to any government USB port
  - Bring USB accessories into a SCIF or Secret open storage space

Reasonable precautions like these may be applied to mitigate the risk of personal fitness devices, even in SCIFs or around Secret open storage.

Personal fitness devices share several key features with other types of personal devices, so consider how these mitigation strategies might apply to those devices, too.

An Example of Risk Mitigation

As a Security Specialist, you are not responsible for making risk mitigation decisions on your own.

If you haven't already, get to know your agency's Information Systems Security Managers, or ISSMs, Information Systems Security Officers, or ISSOs, and other cybersecurity or IT personnel.

These personnel will not only help you coordinate and develop your risk mitigation strategies, you can also seek their input when new technology is introduced in your workplace, and they can help you determine the appropriate response if employees do not follow established procedures.

Review Activity

Jan, a new employee in your organization, uses a wearable medical device that monitors her blood sugar and sends regular updates to her personal smartphone via Bluetooth or a USB connection.

What are just some of the reasonable precautions should you consider before allowing Jan to use her medical device in a secured area?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Ensure the device does not use WiFi or cellular technology
- ☐ Ensure the device does not have recording capability
- ☐ Provide training so that Jan knows she cannot bring USB devices into secure areas
- ☐ Require authentication before Jan may access her device's data

Summary

Congratulations! You have completed the Cybersecurity and the Use of New Personal Devices Short.

Remember, even though technology changes rapidly, fundamental risk mitigation principles still apply and these principles provide a foundation for dealing with new capabilities. For more information, consult DoDD 8100.02 and DoDM 5200.01v3.

Answer Key

Jan, a new employee in your organization, uses a wearable medical device that monitors her blood sugar and sends regular updates to her personal smartphone via Bluetooth or a USB connection.

What are just some of the reasonable precautions should you consider before allowing Jan to use her medical device in a secured area?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☑ Ensure the device does not use WiFi or cellular technology (correct)
- ☑ Ensure the device does not have recording capability (correct)
- ☑ Provide training so that Jan knows she cannot bring USB devices into secure areas (correct)
- ☐ Require authentication before Jan may access her device's data (distractor)

Feedback*: Among other considerations, you should ensure the device does not have WiFi or cellular technology, or recording capabilities. You should remind Jan that USB devices are not permitted in secured areas.*