Bring Your Own Device

BYOD

In this reading, you will learn about a business practice called “bring your own device” (BYOD), as well as the security risks related to BYOD policies and how to mitigate these risks. Organizations can reduce IT costs by limiting the number of company-owned mobile devices issued to employees. Instead, businesses are passing on the costs of mobile devices and cellular services to employees by allowing employees to bring their own devices for business use.

Bring your own device (BYOD)

Traditionally, IT departments would provide mobile devices to employees for business use. This gave the IT staff control over the security of those devices. Today, an increasing number of companies permit employees to bring their own devices to work. This trend started with employees requesting permission to carry a single smartphone rather than carrying one phone for work and one for personal use. Organizations noticed the cost savings gained by allowing their employees to select their personal smartphones as the single device. By using smartphones with dual SIM card slots or phone apps like Google Voice, users can configure multiple phone lines on a single smartphone. However, BYODs can become dangerous security threats to companies’ data and networks. IT departments do not have the same level of control over the security of BYOD devices as they would with company-owned devices.

BYOD Threats

Some of the potential threats BYODs pose to company networks, resources, and data include:

- **Loss or theft** could result in an organization’s data being stolen or the lost device being used to gain unauthorized access to a company’s network.
- **Data loss**, including:

1. **Data leakage** losses can happen when a computing device is lost or compromised; when an employee accidentally saves or sends confidential information to the wrong destination; when a disgruntled employee exposes data maliciously; or when viruses, malware, phishing attacks, etc.

penetrate organizations' networks.

2. **Data portability** losses can occur when former employees take company data with them on their BYOD when they resign or are fired by the organization.

- **Security vulnerabilities** are any type of weakness in the security of a device or network that provides access for a threat to penetrate the system.
- **Meddler in the middle attacks (MITM)** occur when an attacker monitors the data transfers between two sources with the intent to copy and/or interfere with that information. One of the most common opportunities for an MITM attack arises when a mobile device accesses important information through a public Wi-Fi connection, such as at a hotel or restaurant.
- **Malware** is malicious software that can be used to steal, modify, or delete data. It can also be used to gain unauthorized access to a device or network.
- **Jailbreaking** happens when a manufacturer's protective restrictions are removed on a mobile device. Without these restrictions, a device becomes vulnerable to the risk of the user unknowingly installing malicious software.

Solutions

To mitigate these threats, organizations and their IT departments should design security policies for BYOD use inside company networks. Some preventative steps could include:

1. **Develop a bring your own device (BYOD) policy:** IT departments and organizations can create written policies that detail the minimum technology requirements for permitted BYODs, provide instructions for employees on how to properly secure their devices, and list the rules for safe data access and storage.
2. **Use Mobile Device Management (MDM) software:** MDM software can be used to enforce BYOD policy requirements for mobile devices to help secure company data and networks. IT departments can use MDM software to:
    a. Automatically install apps and updates, including antivirus and anti-malware software
    b. Configure secure connections to an organization's wireless networks
    c. Encrypt storage on devices
    d. Require a lock screen and password
    e. Remote wipe a mobile device that is lost or stolen
    f. Block the execution of certain apps
    g. Meet compliance standards
    h. Prevent data being shared or stored in unauthorized locations

i. Manage devices remotely

3. **Use an Enterprise Mobile Management (EMM) system:** MDM policies are specific to mobile operating systems. In order to distribute MDM policies across Android, iOS, and other mobile operating systems, the BYODs can be enrolled through an Enterprise Mobility Management (EMM) system.
4. **Require the use of multi-factor authentication (MFA):** Users can be authenticated by presenting more than one method of identification. Some common identification factors include:
    a. **Something you know**: a password or pin number
    b. **Something you have:** a physical token, like an ATM or bank card, USB device, key fob, or OTP (one-time password)
    c. **Something you are**: biometric data, like a fingerprint, voice signature, facial recognition, or retina scan
    d. **Somewhere you are**: location-dependent access, like a Global Positioning System (GPS) location
    e. **Something you do**: gestures, like swipe patterns; Turing tests, like CAPTCHA; or normal patterns of behavior, like regular login and logout times
5. **Set an acceptable use policy (AUP):** Organizations could create policies that set a code of conduct for use of the companies' data, systems, network, and other resources.
6. **Use non-disclosure agreements (NDA):** Organizations can create legally binding contracts with employees to assert the confidentiality and security policies for the companies' data and intellectual property.
7. **Restrict data access**: IT departments should protect company data by limiting access to only those employees who need access to perform their jobs.
8. **Educate staff about data security:** Organizations can provide training manuals and seminars to inform employees about network security risks and to instruct on how to secure their BYODs.
9. **Back up device data:** IT departments need to create backup policies for all important data. This should include a schedule for frequency of backups, storage space for the back-up copies, how long back-ups should be stored, and disaster recovery plans.
10. **Data leakage prevention (DLP):** IT departments can implement DLP software solutions to help manage and protect confidential information.

Key takeaways

Organizations are taking advantage of the cost savings created by adopting “bring your own device” (BYOD) policies for employees. However, permitting employees to connect personal mobile devices to company networks introduces multiple security threats. There are a variety of security measures that IT departments can implement to protect organizations’ information systems:

- Develop BYOD policies
- Enforce BYOD policies with MDM software
- Distribute MDM settings to multiple OSes through EMM systems
- Require multi-factor authentication (MFA)
- Create acceptable use policies for company data and resources
- Require employees to sign NDAs
- Limit who can access data
- Train employees on data security
- Back up data regularly

Resources for more information

- BYOD (bring your own device) - Additional information on how BYOD works, why is it important, level of access options, risks, challenges, policy comparisons, best practices, how to implement a BYOD policy.
- BYOD policy: An in-depth guide from an IT leader - Compares BYOD advantages and disadvantages, what should be included in a BYOD policy, tips for reducing security risks, and more.
- What is MDM? - Introduces the purpose of MDM software, how it works, advantages of using MDM, use cases, and more.
- Enterprise Mobility Management (EMM) - Outlines the features, services, and benefits of EMM systems.