SECURITY CONSIDERATIONS FOR MOBILE DEVICE DEPLOYMENTS

JUNE 2020 ITSAP.70.002

When selecting an approach to deploy mobile devices in your organization, you can choose from different deployment models, each of which comes with its own benefits and risks. With mobile devices, managing risk depends partly on employee cooperation (i.e. willingness to allow use restrictions, monitoring, and security access by the organization) and partly on the inherent risks and vulnerabilities in the types of devices included. To select a deployment model that best balances these elements for your organization, consider user experience, privacy, and security requirements.

DEPLOYMENT MODELS

Corporately owned, business only (COBO): Your organization owns the device, and it can only be used for business purposes.

Corporately owned, personally enabled (COPE): Your organization owns, controls, and monitors the devices. With this model, your organization can enforce stricter security policies. Employees can use their devices for personal purposes, and you might let them choose the type of device used.

Bring your own device (BYOD): Employees use their own devices for business purposes, and you may choose to cover some of the costs associated with the devices. However, because your organization does not own the device, it has little control over the security controls implemented on the device.

BENEFITS AND RISKS

There are benefits and risks associated with each of these different deployment models. The two tables below list some examples of benefits and risks to consider and whether they apply (✓) or don't apply (**x**) to the deployment model.

However, these benefits and risks may vary based on your organization's security needs and requirements, as well as your users. When considering the benefits and risks of a deployment model, you should also consider which deployment model will enable your organization to balance functionality, user experience, and security.

EXAMPLES OF BENEFITS	COBO	COPE	BYOD
Improve workplace satisfaction	✓	✓	✓
Promote job efficiency and flexibility (e.g. remote work)	✓	✓	✓
Offer device for business and personal use	x	✓	✓
Decrease hardware costs	x	x	✓
Control device updates	✓	✓	x
Providing the option to work remotely	✓	✓	✓

EXAMPLES OF RISKS	COBO	COPE	BYOD
Lack management control (e.g. little control over software updates and downloads)	x	x	✓
Download malicious applications (e.g. hackers gaining access to corporate data)	✓	✓	✓
Use devices insecurely (e.g. access information on public Wi-Fi or letting other people use the device)	✓	✓	✓
Tamper with security features (e.g. jailbreaking a device might unlock configuration restrictions)	x	x	✓
Lose data (e.g. mixing personal and business data can open opportunity for content leakage)	x	✓	✓

RISKS MITIGATIONS

There are many ways to reduce the risks that mobile devices introduce to your organization. Some deployment models allow more room for mitigations than other models.

Most risks for BYOD are uncontrollable because the device is personally owned. With corporately owned devices, you can better manage the risks. In a COBO model, the device is used solely for business purposes, and your organization has complete control over the data on the device and the security policies used. A COPE model offers some of the positives of both BYOD and COBO models; employees can use devices for personal use, but your organization controls the security measures implemented.

The table below lists example mitigations and which deployment model they apply to (✓) or don't apply to (x).

EXAMPLES OF RISK MITIGATIONS	COBO	COPE	BYOD
Enforce the use of strong passwords and authentication mechanisms for devices	✓	✓	x
Ensure security controls are established (e.g. unified endpoint management [UEM])	✓	✓	x
Limit the information shared between devices	✓	✓	x
Offer IT support for devices	✓	✓	x
Use software developed or specifically associated by the organization	✓	✓	x
Access work-related applications using the corporate network infrastructure	✓	✓	✓
Establish an employee exit plan (i.e. devices and data are managed when an employee leaves)	✓	✓	x

UNIFIED ENDPOINT MANAGEMENT (UEM)

Your organization can use UEM to maintain the security of mobile devices. If you support BYOD, you can use UEM, but your ability to manage the devices is minimal because the devices are owned by the employees. In a COPE or COBO model, you can use UEM because you maintain full control of monitoring and securing the devices.

UEM is a strategy to distribute, manage, and control endpoint devices (e.g. desktop and mobile) in the workplace. UEM combines features from mobile device management and enterprise mobility management processes to address security concerns related to managing corporate data while increasing connectivity and productivity. UEM includes features that help keep company information and employee data secure:

- Monitoring devices consistently (e.g. in-office or remotely)
- Separating application platforms (e.g. sandboxing)
- Enforcing strong authentication credentials (e.g. using different keys between personal devices and desktops)
- Incorporating email and messaging services
- Configuring devices for set-up and enrollment
- Encrypting data at rest and in transit
- Performing remote tracking, locking, and wiping
- Detecting jailbroken or rooted devices
- Updating security patches and anti-malware software automatically
- Whitelisting and blacklisting applications

CONSIDERATIONS FOR YOUR ORGANIZATION

Your organization should choose the deployment model that best suits business needs through considering the following:

- Level of control needed depending on the sensitivity of the data being handled.
- Budget available for specific deployment models (e.g. hardware supply, IT support).
- Best balance between business and personal life.

It is important that your organization trains employees on best privacy and security practices to ensure safe use with the deployment model your organization uses.

Need help or have questions? Want to stay up to date and find out more on all things cyber security? Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**