Security considerations for mobile device deployments

CANADIAN CENTRE FOR CYBER SECURITY

October 2024 | ITSAP.70.002

When determining how 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 and their willingness to accept user restrictions, monitoring and security access by the organization. It also depends on the inherent vulnerabilities in the types of devices in question. To select a deployment model that best balances these elements for your organization, consider user experience, privacy, and security requirements.

Mobile device deployment models

Listed below are the following mobile device deployment models along with the benefits and risks associated with each:

- Corporately owned, business only (COBO)
- Corporately owned, personally enabled (COPE)
- Bring your own device (BYOD)

Note that the benefits and risks may vary based on your organization's security needs and requirements, as well as your users. When choosing a deployment model, you should also consider which one will allow your organization to balance functionality, user experience and security.

Corporately owned, business only

In the COBO model, your organization owns the device which employees use only for business purposes. COBO allows an efficient business-only workflow and provides secure remote work, standardized device management, support, and maintenance, including updates. With COBO, your organization has full control of security policies, including password complexity, data encryption, access restrictions, and vulnerability management.

Benefits of the COBO model include:

- increased job efficiency and flexibility
- ability to control device updates
- the option for remote work
- no risk of malicious application download as your organization can limit the applications to only those it has evaluated for security and business value

Risks of the COBO model include:

- overly restrictive configurations for COBO may increase risk if employees feel that corporately issued devices restrict their ability to work efficiently and opt to use personal devices
- reduced flexibility for employees as they can only use a limited selection of curated apps
- vulnerabilities associated with relaxing restriction to allow connections to Bluetooth, public or other untrusted Wi-Fi, USBs or other removable storage
- vulnerabilities linked to split tunneling of VPNs where some application or device traffic is routed through an encrypted VPN, while other traffic has direct access to the Internet

Corporately owned, personally enabled

With the COPE model your organization owns, controls, and monitors the devices and can enforce stricter security policies. A COPE model offers some of the positives of both COBO and BYOD models. Employees can use devices for personal use, but your organization controls the security measures implemented. Should you allow employees to choose their own device, the cost may be higher. You will need to evaluate and procure multiple devices, develop multiple support procedures, and navigate varying levels of security controls provided by different manufacturers.

Benefits of the COPE model include:

- greater workplace and employee satisfaction
- increased job efficiency and flexibility
- ability to control device updates
- option for remote work

Risks of the COPE model include:

- use of untrusted apps and networks
- poor user cyber hygiene and risky Internet practices
- lack of email filtering and internet browser filtering
- intentional tampering with security controls
- lack of audit and monitoring controls
- malicious application downloads, enabling hackers to access corporate data
- lost data, as mixing personal and business data can create an opportunity for content leakage
- relaxation of strict security controls in favour of usability or other business or executive requirements

Bring your own device

The BYOD model allows employees to use their own devices for business purposes. You may also choose to subsidize some of the associated costs. However, because your organization does not own the device, you have little control over the security measures implemented on the device. The risks of this model are the same as the COPE model, but with fewer security controls available.

Benefits of the BYOD model include:

- greater workplace and employee satisfaction
- increased job efficiency and flexibility
- the option for remote work
- business and personal use
- lower hardware costs

Risks of the BYOD model include:

- ability of the organization to mitigate any compromises is extremely limited as it does not own the device
- malicious application downloads, enabling hackers to access corporate data
- insecure device use, as users may access information on public Wi-Fi or allow others to use the device
- lost management control over software updates and downloads
- tampering with security features and unlocking configuration restrictions
- lost data, as mixing personal and business data can create an opportunity for content leakage

AWARENESS SERIES

Cat. No. D97-1/70-002-2024E-PDF ISBN 978-0-660-73534-4

Canada

Risk mitigations for mobile device deployments

There are many ways to reduce the risks that mobile devices introduce to your organization. Both the COBO and the COPE models allow for the following risk mitigations:

- enforcing the use of strong passwords and authentication mechanisms for devices
- establishing security controls
- limiting the information shared between devices
- offering IT support for devices
- using software developed or specifically purchased and verified by the organization
- accessing work-related applications using the corporate network infrastructure
- managing devices and data when an employee departs

The only concrete risk mitigation that the BYOD model provides is the ability to use the corporate network. Most risks for BYOD are beyond corporate control because the device is personally owned.

Considerations for mobile device deployment

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

- level of control needed depending on the sensitivity of your information
- budget available for specific deployment models, including hardware supply and IT support
- best balance between business needs and workplace satisfaction

Unified endpoint management

Unified endpoint management (UEM) is a strategy to distribute, manage and control endpoint desktop and mobile devices 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 your organization's information and employees' data secure, such as:

- monitoring devices consistently, in office or remotely
- separating application platforms, also known as sandboxing
- enforcing strong authentication credentials
- incorporating email and messaging services
- configuring devices for set-up and enrolment
- encrypting data at rest and in transit
- performing remote tracking, locking, and wiping
- detecting when users remove security permissions
- updating security patches and anti-malware software automatically
- allow listing and deny listing applications

Your organization can use UEM to maintain the security of mobile devices. You can use UEM with the BYOD model, but your ability to manage the devices is minimal because the devices are employee-owned. In a COPE or COBO model, you can implement UEM more effectively because you maintain full control of monitoring and securing the devices.

Finally, choose security controls carefully when implementing UEM. It is important to understand what each setting does and its implications to both security and usability. Although tempting, turning on every restriction available may degrade the user experience and render a device much less usable. This may motivate users to intentionally bypass security controls or opt to use less restrictive personal devices, despite knowing that doing so is less secure and against company policy.

Learn more

- End user device security for Bring-Your-Own-Device (BYOD) deployment models (ITSM.70.003)
- How updates secure your device (ITSAP.10.096)
- Mobile devices and business travellers (ITSAP.00.087)
- Mobile device guidance for high profile travellers (ITSAP.00.088)
- Cyber security at home and in the office: Secure your devices, computers, and networks (ITSAP.00.007)
- Security tips for organizations with remote workers (ITSAP.10.016)

AWARENESS SERIES

Cat. No. D97-1/70-002-2024E-PDF ISBN 978-0-660-73534-4

Canada