Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

End user device security for Bring-Your-Own-Device (BYOD) deployment models

MANAGEMENT

Canada

Foreword

ITSM.70.003 End User Device Security for Bring-Your-Own-Device Deployment Models is an unclassified publication issued under the authority of the Head of the Canadian Centre for Cyber Security (the Cyber Centre).

For more information, email or phone or Contact Centre:

Contact Centre
cyber.gc.ca
contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

Effective date

This publication takes effect on April 28,2022.

Revision history

Revision	Amendments	Date
1	First release.	April 28, 2022

Overview

This document introduces potentially vulnerable attack surfaces associated with end user devices that are used as part of bring-your-own-device (BYOD) deployment models in organizations of all sizes. This document also provides mitigation techniques that your organization can apply to reduce the risks if it chooses to implement a BYOD model.

Poorly configured end user devices can put your organization at risk. They are entry points through which threat actors can gain unauthorized access to sensitive data. End users may not have the technical expertise to avoid potential security incidents and rely on technical controls and policies that are inherent to the devices to keep them and their data secure.

If your organization chooses to use a BYOD deployment model, you must be aware that end users can unknowingly introduce additional risk to your environment. Many of the organizational policy controls are soft limitations as opposed to hard restrictions due to the legalities of ownership and, due to the design of the systems supporting them, technical controls are limited on the device side.

ISBN 978-0-660-43392-9

CAT D97-4/70-003-2022E-PDF

Table of contents

1 Introduction

This document introduces potentially vulnerable attack surfaces that are associated with end user devices that are used as part of bring-your-own-device (BYOD) deployment models in organizations of all sizes. This document also provides mitigation techniques that your organization can apply to reduce the risks if it chooses to implement a BYOD model.

BYOD is the practice of allowing staff to bring and use their own personal devices (e.g. phones, laptops, tablets) to access enterprise data and systems for business purposes. BYOD deployment models vary in levels of restriction, from granting users unlimited access to systems and data, to restricting access to only non-sensitive systems and data, or to access with conditions in place (e.g. IT control over personal devices and prevention of local storage of data on personal devices).

When considering whether to implement a BYOD deployment model in your organization, you should examine the associated benefits and the risks to determine whether a BYOD model supports your organization's risk tolerance.

1.1 Is BYOD right for my organization?

We recommend that your organization consider its security and operational requirements when choosing a device deployment model. Where possible, we recommend providing corporately owned devices, as your organization has more control over the security controls and configurations applied on devices. If you choose to implement a BYOD model, you should consider the legal, security, technological, and budgetary factors that may affect the feasibility of the model. For more information on the privacy impact of managing a BYOD device in a corporate environment, please see *Personal Information Protection and Electronic Documents Act (*PIPEDA) [1] and the *Privacy Act* [2].

For an overview of the various mobile device deployment models, see *ITSAP.70.002 Security Considerations for Mobile Device Deployments* [3][1]. For more information on the baseline actions that you can take to protect your networks and information, review *ITSM.10.189 Top 10 IT Security Actions to Protect Internet-Connected Networks and Information* [4] and the *Baseline Cyber Security Controls for Small and Medium Businesses V1.2* [5].

1.2 Attack surface of end user devices

BYOD models introduce various risks to the organization in which they are deployed. Some of these are related to organizational data, and others related to privacy implications. Below you will find a list of the most common risks associated with introducing BYOD:

- **Unauthorized applications:** Unauthorized applications installed on a device can cause security concerns as the integrity, availability, and confidentiality of the organizations' information and systems are at risk. Threat actors can use applications for malicious intent and potentially gain access to device location, network settings, the files, applications, and data stored on the device. Crypto malware can also wreak havoc on the availability and integrity of data.
- **Data leaks:** BYOD devices potentially open the door to confidential or sensitive data being shared or leaked in ways that would not be possible if employees used corporately issued devices. Social Media applications and accounts

[1] Numbers in square brackets refer to resources cited in the Supporting Content section of this document.

are often installed and configured on personally owned devices and allow you to quickly share text, pictures, audio, and video content to a wide, and often public-facing audience. Personally owned devices are not as secure as corporately provided devices. Personal devices allow users to access a variety of apps and websites that would likely not be permitted on a corporately issued device. Accessing some of these apps and websites can expose your organization to additional risks, such as providing threat actors additional vectors to exploit and gain access to your corporate systems and networks. BYOD devices are a target for threat actors, as these devices store a large amount of data and provide an entry point to connected corporate systems and networks. BYOD devices may be more susceptible to privacy breaches than corporate devices that do not contain personal information. Threat actors may steal your data to sell or hold it for ransom.

Users may also connect to unsecure Wi-Fi networks more often with their personal devices. Often, once you have connected your device to these networks, it will automatically reconnect in the future. Users may also download and store large amounts of data offline to avoid waiting or exceeding their bandwidth allotments. Since the device has fewer controls than your organization's infrastructure, there is an increased chance of data leaks.

- **Privacy concerns:** With the ability of most mobile device management (MDM) and unified endpoint management (UEM) software to allow deep insights into the user environment on the device, personal details (e.g. email, personal information stored in applications and files, location, and other aspects of a users' identity) can be accidentally or maliciously viewed. Employees may be hesitant to provide organizational visibility into their device. Given that you have limited abilities to monitor or detect threats, this increases the attack surface.
- **Device sharing:** Devices that are personally owned may be shared with family and friends. This can cause accidental information leaks and could compromise the integrity of any data stored on the device.
- **Device rooting/jailbreaking:** Personally owned devices are sometimes "rooted" or "jailbroken." This means that some of the normal security permissions are removed, giving users and applications more access to the core operating system. These devices have a higher potential to bypass security controls implemented by your organization and put your data, network, and applications at increased risk. To mitigate this risk, you should disallow any device that has been altered beyond its intended use and permissions. It is also important to define what corporate data is permitted on a device used for BYOD purposes via policies and education. Your policies and training should provide employees guidance regarding the appropriate use (e.g. which personal activities are permitted on the device), data protection, and security measures for their devices.
- **Lack of provisioned patching and updates:** If your organization implements a BYOD model, it may limit your ability to provision and update the operating systems, applications, and desktop environments. One method your organization can use to help ensure new security updates are provided is by allowing only approved devices that meet the compliance requirements of the organization (that are patched and supported by the manufacturer) to have BYOD access.

2 Best practices

This section outlines security best practices that your organization can implement to reduce the risks associated with BYOD. In a BYOD model, you can follow general guidelines to secure end user devices, including:

- Implementing policies
- Creating onboarding and offboarding procedures
- Handling data securely
- Applying technical security controls
- Training all employees, including executives, contractors, volunteers, and students

Your organization should ensure its policies and security controls align with its business, security, and privacy requirements. You should have layers of security measures (defence in depth approach) applied to protect the confidentiality, integrity, and availability of your organization's networks, systems, and data.

You should consider the legal and privacy implications of your policies and requirements before implementing them. Some legal considerations may include restrictions on the data used on a BYOD device, such as data that is subject to a non-disclosure agreement (NDA) or data that could expose the privacy of Canadians. Note that the guidance in this document is not legal advice. You should seek advice from a lawyer to ensure that you are following all Canadian laws correctly.

2.1 Implementing policies

Implementing organizational policies standardizes the roles, responsibilities, and expected behaviours of all employees. Your policies should be approved and supported by senior management and executives. Policies can help you define how, why, and when to apply best practices, and they also provide structure around data governance. Your organization should review its policies regularly to ensure they are still applicable and update them as required.

2.1.1 Acceptable use policy

This type of policy clarifies what service, network, system, or website can and cannot be used, for reducing legal liability, and giving users clearly stated parameters. We recommend having new and existing staff members sign the acceptable use policy. Alternatively, you may have them sign a separate document to acknowledge that they have read, understand, and agree to the policy. Your organization may choose to ask employees to sign the document periodically (such as annually) or when changes are made to the policy.

2.1.2 BYOD policy

A BYOD policy should enforce the additional restrictions that apply to devices used in a BYOD deployment model and designate who in the organization can use the BYOD model. The policy should clearly define the organization versus end users' roles in securing data and systems.

Your policy should align with your organization's information management policy, stating the proper way to retain, copy, sync, or dispose of corporate data.

Some examples of items you should address in the policy:

- User responsibilities
- Phone plan responsibility
- Requirements for installing MDM or Mobile Application Management (MAM) software
- Maintaining restricted access to corporate data
- Privacy practices an organization has in effect for personal and corporate use of a BYOD device
- Approved devices, operating systems, software
- Classes of data that can and cannot be accessed, developed, or stored on the BYOD device

The BYOD policy should also define what the sandboxed or containerized environment (defined in 2.4.1.5) on a BYOD device can be used for and how the company can manage the device without overstepping. Rooted or jailbroken devices should not be permitted, as these modified devices have more open permissions that allow more system access while avoiding some security features. MAM, MDM and UEM should also be defined and associated to the types of devices to which each technology is applied.

Mobile Threat Defenders (MTDs) go further and inform you of how risky an application is. These typically come integrated with Mobile Endpoint Protection Platforms (EPP) or Mobile Endpoint Detection and Response (EDR) agents that either are controlled by the administrator's policy or interactively by asking the user if they would like to allow a potentially risky application to run.

2.1.3 Encryption and data security policy

Encryption protects the confidentiality and integrity of sensitive data. Your encryption and data security policy defines the data encryption requirements, the acceptable encryption algorithms, and the parameters that your organization considers secure. It should outline portable media encryption, data at rest, and transport encryption. It should also define a standard depending on the class of data in question.

For our recommendations on cryptographic algorithms, refer to *ITSP.40.111 Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information* [6].

2.1.4 Data governance or information management policy

Data governance is the process of managing the availability, usability, integrity, and security of organizational data.
Your data governance policy defines the roles and responsibilities for managing information in alignment with legislative and regulatory requirements and business needs. This policy ensures data is not misused and conforms to a standard that is enforced throughout the organization. The data governance policy should define the retention and disposition requirements of data, the acceptable destruction methods, and the general lifecycle of data based on its category or classification. It should also define data residency requirements and data controls.

2.1.5 Authentication policy

An authentication policy defines your organization's requirements for a secure and acceptable workflow for device, application, and container authorization. For low sensitivity environments, following minimum password best practices might be considered enough. For organizations that collect and retain sensitive information, such as medical or financial, the requirements should be much greater due to the enhanced confidentiality and security requirements of the systems and data to which authorized individuals have access. Multi-factor authentication (MFA) should be implemented where possible and a Role Based Access Control (RBAC) model should be used for BYOD devices. The organizational policy should define what the expiration periods are, whether passwords can be reused, who can reset or change a password, and how credentials are to be securely stored.

For additional best practices, see *ITSAP.30.032 Best Practices for Passphrases and Passwords* [7].

2.1.6 Patching policy

Everyday there are new exploits discovered that put endpoints at risk. To protect against these exploits and cyber threats, you should update all device operating systems and applications regularly and install security patches. Your patching policy defines your organization's strategy for patching, such as what is patched. Examples include mobile device or computer operating systems, applications, anti-malware or anti-phishing systems, and network equipment. The policy should also define the processes for identifying, acquiring, testing, installing, and verifying patches. You should identify who is authorized to perform patching processes and who needs to be notified, if a patch fails, and within what window of time.

There are difficulties associated with patching BYOD devices because they are owned and managed by the end user. You need to determine how you will address patching requirements and potential security vulnerabilities on personal devices. A common target for modern attackers is kernel mode, which allows low-level and complete access to your device. To mitigate the many security vulnerabilities that exist with the kernel or kernel mode, patching is required.

For information on patching, see *ITSAP.10.096 How Updates Secure Your Device* [8].

2.1.7 Public Wi-Fi policy

You should have either a dedicated policy, or a section within another policy, that defines whether public or untrusted Wi-Fi networks, such as at a coffee shop, hotel, or unmanaged networks, may be used. This may include requirements such as using a corporate virtual private network (VPN), limiting access to less confidential classes of data, or following additional precautions to prevent threat actors from eavesdropping and obtaining data.

For best practices regarding Wi-Fi and VPNs, see *ITSAP.80.009 Protecting Your Organization While Using Wi-Fi* [9] and *ITSAP.80.101 Virtual Private Networks* [10].

2.1.8 Incident management policy

An incident management policy should include how any security, privacy, or data leaks are dealt with from an organizational perspective. It should detail how breaches are detected, contained, reviewed, mitigated, and reported. Given the nature of BYOD, this comes down to the owner of the device being technically savvy enough to notice a breach (or the breach occurring within a corporate application), and the end user reporting the incident. The policy should outline the responsible

parties for each element and should be covered during training. Often, a security incident may require a drastic measure such as complete erase and wipe of a device, which most users will be unwilling to do on a personally owned device. This policy should be reviewed often and tested to ensure it remains up to date.

2.2 Creating onboarding and offboarding processes

You should have clearly defined processes and procedures for onboarding and offboarding BYOD devices in your organization's environment.

As per your organization's BYOD policy, you may only allow certain devices to be onboarded. You should ensure that all end users have read and understand their roles and responsibilities as per all the organization's policies. When onboarding, you should ensure that you do the following activities:

- Track all devices in an inventory
- Scan them for malicious software (malware) and applications using an MTD
- Advise the users of the requirement and policies of securing the devices with an authentication mechanism that meets the organization's policy
- Use allowlisting for approved BYOD during onboarding process
- Enable encryption on the device, container/sandbox, and communications channels utilized for organizational purposes such as for email, and applications
- Patch and mitigate any software vulnerabilities that may be present on the device

When offboarding, you must ensure that company-specific data is wiped from the device and access is removed to any company resources to prevent data breaches and leaks via unmanaged devices. Given that the device is personally owned rather than corporately owned, a full wipe should not be performed unless the user consents, as it would erase the personal data of the owner. If possible, use a "selective wipe" to only wipe the data associated with the work account. For information on sanitization, see *ITSAP.40.006 Sanitization and Disposal of Electronic Devices* [11] and *ITSP.40.006 IT Media Sanitization* [12].

For any employee who is switching roles within your organization, you should review any information stored on their device and re-evaluate if there is a need-to-know. Any data or applications that are no longer relevant for the employee's new role should be removed. This is another measure in which you can ensure your high value data is protected.

2.3 Protecting and handling data securely

Protecting and handling data in a secure manner ensures that any security incidents or malicious activity that occurs on an application, device, network, or system is limited within the zone or grouping of the security boundary. There are four key actions your organization can take to enhance the security of your data.

2.3.1 Classifying data

Classifying data ensures that sensitive data never leaves an area where it cannot be protected and limits the potential damage of a data breach. This is achieved by applying class-specific controls based on the required level of confidentiality,

integrity, and availability of data. Data should be structured based on organizational, privacy, and security requirements. Below, we provide an example method for how you may want to categorize your data. Government of Canada (GC) departments and agencies should follow the GC's data classification requirements.

An example method of structuring these classes is provided below:

Class 1: Public data

This class of data is used to define data that is accessible and available to the public. No harm would be done to the business or the clients, staff, and vendors with this data being handled internally and externally. Some examples of public data include company public webpages, brochures, and business cards.

Class 2: Internal-only data

This type of data is only meant to be used inside the company with authorized personnel. Internal-only data contains slightly sensitive information (e.g. not including personal identifiable information (PII)) about the organization's operations, policies, or business plans. Some examples are internal memos and business-related emails. If this data were to get out to those without authorization it could pose minimal harm to the business.

Class 3: Confidential data

This data is limited to a specific group within the organization who hold a special clearance or clear permissions to use and access this data. Confidential data may contain PII that would cause great harm to the organization, individuals, and parties involved if compromised. Typically, this data is protected by the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA) or is regulated under as the Investment Industry Regulatory Organization of Canada (IIROC) or the Mutual Fund Dealers Association (MFDA) of Canada. Examples of this data include proprietary business data, research data, source code to software, intellectual property, and other PII.

The examples listed above are only a few ways in which you can classify your data. For a more complete list and additional information, please refer to the PIPEDA [1] and the Privacy Act [2].

Even with policies and security controls in place, residual risk always remains. To reduce the risks associated with compromised end user devices, your organization should limit the information that can be accessed, stored, or synced by personal devices. For example, you may need email messages to sync to the device for offline viewing, but you should not sync the entire mailbox; a user's inbox should only display recent emails (within few weeks). End users should not be able to access systems that contain sensitive data, such as logins or social insurance numbers (SIN), when using personal devices. Instead, they should only be allowed to access non-sensitive information.

You should refer to your data class structure when determining the information that personal devices can access, store, or sync. Keep in mind that many services access from mobile devices are now in the cloud, and therefore the data may or may not get stored locally, such as in an offline cache.

2.3.2 Network segmentation

You should segment your organization's networks into various security zones. A zone is a well-defined perimeter with connection points. Zones have various levels of sensitivity and contain different classes of data. If you implement a BYOD deployment model, you can use network segmentation to reduce your attack surface and the potential risks of unauthorized

access or data disclosures. Network segmentation will not protect cloud-based services from mobile device access directly, only services available on your local network.

For more information on network segmentation, refer to *ITSP.80.022 Baseline Security Requirements for Network Security Zones* [13] and *ITSG-38 Network Security Zoning – Design Considerations for Placement of Services within Zones* [14].

2.3.3 Isolating corporate data from personal data

As mentioned previously, limiting data access to a need-to-know basis will help reduce the attack surface for a threat actor if an account or system is compromised. An integral part of protecting corporate data is ensuring there is sufficient separation between your corporate data repositories and personal data. The following are some considerations for data separation when deploying BYOD in your organization. Many of these can be accomplished using an MDM/UEM or MAM along with an MTD.

- Contacts
- Short Message Service (SMS)/Multimedia Messaging Service (MMS)
- Email accounts
- Social media accounts
- Application access (personal and corporate application interaction capabilities)

2.4 Applying technical security controls

While policies help govern the regulations that are applied organization-wide, technical controls help enforce the policy requirements. Technical controls are deployed with software or hardware to prevent security incidents or reduce the harm should an incident occur. These controls can be automatic or part of a manual process.

To properly implement the technical controls that your organization requires, you may require additional technical support.

2.4.1 End device controls

2.4.1.1 Device management

MDM, MAM, or UEM can provide visibility, apply technical controls and policies, and limit the types of attacks used to put security at risk. The MDM/UEM or MAM server software can be cloud-hosted, self-hosted, or provider-hosted, depending on your organization's requirements. Some device manufacturers include built-in methods to connect a device to an MDM. However, typically third-party software is used to implement the full functionality provided by the chosen product.

MAM only controls applications on the device and will not consistently enforce device-wide policies. Typically, MAM is used to control features within an application, force more secure defaults, or isolate business applications from personal applications.

MDM/UEM ensures that diverse hardware can be configured consistently and reliably through automated means. It may limit functionality in favour of a more secure environment, install needed applications or features, and assist in troubleshooting and diagnosing problems with devices. In a BYOD environment, there is little an organization can impose on MDM/UEM

software as it should only affect the corporate apps, not the entire device itself (exceptions include: whole-device password, and an auto-lock timeout). Many MDMs can also restrict rooted or jailbroken devices from connecting.

2.4.1.2 Anti-malware and MTD/EPP

Anti-malware is software that combats malicious pieces of code. We highly recommend anti-malware for not just corporate devices, but also personal laptops and desktops, as it provides a layer of confirmation that the device is not infected. Given that the prior state of a BYOD device is not known, devices should be scanned before they are allowed to connect and consistently during their continued use.

Regularly update definitions to ensure that the software maintains the most recent database of signatures and heuristics to catch as many malicious applications as possible.

You should schedule scans if they are not automatically configured by the anti-malware software. Scheduled scans ensure that if the real-time scanner misses any malicious software, or if the software was placed on the device through an unmonitored vector, it will be found.

Keep in mind that anti-malware software is not the first line of defence; it is merely there to catch things that fall through the cracks.

Mobile devices such as cell phones and tablets should use MTD/EPP agents to ensure mobile security, as anti-malware alone is not effective on these platforms. MTDs and EPPs are beneficial not only for the organization but also for the owner of the device and can be anonymized to avoid any privacy concerns.

2.4.1.3 Applications and permissions

Typically, applications are vetted initially by either the Google Play Store or Apple App Store if applications are installed from one of these sources. However, you should not rely solely on this initial vetting process. MDM, and UEMs can further vet the corporate application based on the specific application itself and your organization's security needs. For example, an MDM can help regulate trusted and vetted applications that are permitted for use on the organization's workspace on the mobile device (refer to Sandbox Frameworks in section 2.4.1.5 below), and policies surrounding BYOD devices or mobile devices should help define the requirements around surrounding which applications or types of applications are permitted.

When vetting applications, you should consider the permissions that applications have and ensure they only have the permissions required. For example, a calculator application should not need to access the GPS location or contacts unless there is a feature in the application that supports it. Always review what access an application is requesting before granting that access.

Permissions to corporate contacts should not be allowed from the personal sandbox environment of the device (refer to Sandbox Frameworks in section 2.4.1.5 below); untrusted applications on the personal sandbox could access and compromise contact information or other sensitive information (e.g. PII). Typically, a sandbox, MDM, or UEM solution implements a separate contact list for corporate use.

Your organization should not allow rooted or jailbroken mobile devices on your corporate network, as these devices can bypass some built-in security features and permissions.

2.4.1.4 Security policies

You should enforce your written policies through a variety of technologies, such as security policies, ACLs, MDM/UEM, MAM, and MTD. With security policies, you can restrict features, or how they are used, and enforce secure algorithms, password entropy, and applications that can be installed, among many other variables. Typically, you apply security policies on the infrastructure side of the network through an MDM or endpoint management solution, and the end device enforces it.

MDM will enforce device-wide security policies, such as password entropy and allowed applications. A MAM will enforce application specific policies, such as features that can be used or the ability to copy and paste data. Typically, MAM deals with more fine-grained controls within applications, as opposed to broad, higher-level restrictions placed by the MDM.

2.4.1.5 Sandbox frameworks / containerization

A sandbox is an isolated environment which limits access to and from other applications and resources of the sandboxed environment. Sandboxing on a BYOD device is especially important because the device contains both personal and work-related data and applications. Without sandboxing, a user could install a malicious application (whether it be by accident, or intentional) that, in some circumstances could potentially access confidential data stored in or interfere with an app used for work. There is no guarantee that resources can remain securely separated with a sandbox, and with BYOD the personal owner can intentionally, or unintentionally weaken the security of the sandbox, therefore it is important that the host OS is kept secure by the owner of the device.

Examples of sandbox frameworks include Samsung KNOX, Kiosk software, Apple App Sandbox, and a dedicated read-only/locked Virtual Machine (VM). Some features of these frameworks are already active on stock configured endpoint devices but become more useful when paired with an MDM/UEM and/or MAM solution.

It is common for sandboxing frameworks to cause additional steps or minor inconvenience to the end user, such as requesting additional permissions or authorization of a user, application, or code. Due to this, you should ensure that all users understand why certain technical controls are in place and how they impact security.

2.4.2 Infrastructure controls

2.4.2.1 Domain Name System (DNS) filtering

DNS is used for all Internet-connected devices to translate text to an IP Address, and it plays a large part in connecting you to the resources you need. You can use a DNS to filter out malicious hosts and prevent you from being directed to a malicious website.

Internet service providers (ISPs) offer their own public DNS servers, but we recommend using an alternative DNS service for extra privacy, performance, and security. Other organizations also offer free public DNS services that filter DNS requests from malicious websites, hosts, systems. The Canadian Internet Registration Authority (CIRA), which is a not-for-profit agency that manages the dot CA Internet domain, offers a free protected DNS service called Canadian Shield.

2.4.2.2 Mobile behavioural analysis

This technique analyzes events that occur on a device, network, system, or service. In respect to BYOD, this is typically limited to any corporately controlled devices, networks, systems, and services. For example, with behavioural analysis, you

can detect when a mobile device suddenly pulls all employee records in an application that normally accesses only a few records in a short period or when a device tries to connect to thousands of Transmission Control Protocol and User Data Protocol (TCP/UDP) ports on a network within a short timeframe. Network based monitoring should be combined with applying access-based controls (such as ACLs) and limiting the amount of data that can be downloaded to a BYOD device.

Some examples of mobile behavioral analysis systems include intrusion detection systems (IDS), intrusion prevention systems (IPS), or security appliances and/or applications that use artificial intelligence to analyze common usage patterns and report abnormalities. MTDs are commonly used with integrated Mobile EPP and Mobile EDR components that allow an evaluation of an application to be performed and either; through user interaction or automatic rules, permit or deny an application to perform an action.

2.4.2.3 Anti-phishing and anti-spam

Anti-phishing and anti-spam technologies are critical for protecting your organization's email domains. Some common standards used for email domain protection include pointer records (PTR), DNS, Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-Based Message Authentication, Reporting, and Conformance (DMARC) records.

Additionally, you may choose to use a signature and heuristics-based anti-spam service. Typically, these services also provide anti-malware services for in-transit messages and filter based on specified rules. While many of these applications work at the infrastructure level, you can also find security suites or anti-malware software that comes bundled with them for desktops and laptops. Mobile devices such as cell phones cannot easily detonate malicious executables on-device so these platforms generally exclusively use the infrastructure supplied solutions.

No software or solution is perfect, but a good solution can greatly decrease the amount of inbound spam and malicious emails that end users see, reducing the risk of compromises.

For more information on protecting your organization's domains from email spoofing, see *ITSP.40.065 Implementation Guidance: Email Domain Protection* [15].

2.4.2.4 Access control lists and sensitivity of data

On platforms that support them (desktops, laptops), access control lists allow you to define the permissions that a group or specific user has for organizational resources (e.g. network drive, an email inbox, administrative functions). If using a BYOD deployment model, you need to define access that devices have. You should apply the principle of least privilege to ensure that individuals only have access to the resources and information they need for their job functions. Limiting access reduces the attack surface and potential harm if a device is compromised.

For example, you could set up a secure perimeter on the network to ensure that only corporately owned devices have access.

2.4.2.5 VPNs

A VPN is a secure connection between two points, such as a laptop and your organization's network or between an application and a server. The VPN acts as a tunnel that you can use to send and receive secure data on an existing physical network. When using a VPN, data is encrypted during transmission so that, if intercepted, attackers cannot directly see the data without the decryption key.

There are several different types of VPNs that are applicable to BYOD:

- **Host-to-gateway (remote access):** Provides remote access from a device to an enterprise network. This is the most common method used in a corporate environment for users to connect into the resources they need for work. Multi-factor authentication (MFA) should be used to secure the connection to this service and split-tunneling should be avoided when possible. Split-tunneling is the ability for a host to use both its direct internet connection and the remote network simultaneously.
- **Host-to-host:** Connects a host to a specific resource on an enterprise network or another specific host.
- **Application to Server or Zero Trust Network Access (ZTNA):** Some modern applications create a private Transport Layer Security (TLS) tunnel between themselves to their server, providing a secure connection to transfer data, outside of a standard VPN tunnel. ZTNA is also used for application-level or for a group of applications to form an identity and context-based border. This technology authenticates each application and user to ensure the need-to-know principle is followed. While traditional VPNs allow network access, ZTNA connections do not allow network visibility by default.
- **Third-party privacy:** Secures a connection from a public access point (e.g. airport or hotel Wi-Fi hotspot) to a third-party VPN provider and redirects the user's traffic to make it appear to originate from the third-party's network. Third-party privacy is not recommended for corporate use as it does not provide any true end-to-end security or privacy beyond the local network.

If you have employees who are working remotely and must use unsecured or public networks, they should use a VPN or ZTNA micro tunnels to establish a secure connection that uses authentication and protects data. Authentication can be done via certificates or traditional credentials as well as requiring multi-factor authentication.

For more information on VPNs, see ITSAP.80.101 Virtual Private Networks [10].

2.4.2.6 Cloud environments

Cloud environments provide a low-entry barrier for smaller organizations to take advantage of more sophisticated security controls that can help secure BYOD devices in a cost-effective manner. By using a cloud environment, you can benefit from security features that are developed and managed by large teams working for the cloud service provider and that may otherwise be unavailable or require significant financial investment. There are fewer consequences if a cloud service is compromised from an end user device, as the threat actor will not have access to the data stored outside the device. However, even if you use cloud services, your organization is still legally responsible for protecting its data.

2.5 Training employees

Training is an essential part of your organization's cyber security and enhances your organization's overall cyber security by empowering employees on their personal cyber security practices. Any person who has access to your networks, systems, devices, and information should understand their roles and responsibilities with regards to cyber security. Training gives you the opportunity to familiarize your employees with your policies and the basics of security (e.g. identifying phishing messages, enabling multi-factor authentication, working safely from home, reporting security incidents, and privacy breaches).

In the context of BYOD models, your organization should educate your employees on the systems available on personal devices, the classes of data that can be stored on personal devices, mobile application training, the retention and disposition schedules of corporate data, their access permissions, guidance on how they can secure their personal devices, and appropriate disclosure practices. BYOD technical controls and policies should be introduced as ways to help improve organizational awareness, consistency, and security.

Users should have access to policies, playbooks, or procedures that specify how they are to interact with systems and data while maintaining security. You should review these policies and instruments on a regular basis and update when required.

There are various security courses offered online that can help improve general mobile security knowledge. This training should focus on how to be secure on a mobile device such as a laptop, cell phone, or tablet and how to deal with security prompts that may show up or common misconceptions about mobile security. The Cyber Centre's Learning Hub offers in-class and online learning activities and programs for various audiences, including non-technical employees, IT practitioners, and senior level managers. Currently, these activities and programs are offered primarily to those who work within the Government of Canada (GC) or with our domestic partners; however, provincial, and municipal governments and organizations, as well as industry partners who work with GC departments may also participate.

All Learning Hub courses can be delivered organization-wide or to individual employees or small groups. Courses cover topics including:

- IT security risk management
- Cyber security for developers and IT practitioners
- Communications security
- Cryptographic security

Course offerings may change, but you can review the Learning Hub course calendar on our website for more information on available courses.

The Privacy Awareness Training [16] offered by the GC is also a great resource for understanding privacy commitments including risk management and compliance.

For more information on training, see *ITSM.10.093 Top 10 IT Security Actions: #6 Provide Tailored Cyber Security Training* [17].

3 Summary

There are benefits and risks associated with any mobile device deployment model. However, some deployment models allow more room for mitigations than other models. Most of the risks associated with BYOD are uncontrollable because the devices are personally owned. With corporately owned devices, you have more control over the data on the devices and the technical security control that are implemented.

If you choose to implement BYOD, your organization should conduct a risk assessment and ensure that there are policies and technical controls in place to reduce the risks to a tolerable and accepted level. You should also consider the additional support and legal implications associated with BYOD and the technical controls that you implement.

4 Supporting content

4.1 List of abbreviations

Term	Definition
BYOD	Bring your own device
CSE	Communications Security Establishment
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain name system
EDR	Endpoint Detection and Response
EPP	Endpoint Protection Platform
GC	Government of Canada
IIROC	Investment Industry Regulatory Organization of Canada
IDS	Intrusion detection system
IPS	Intrusion prevention system
ISP	Internet service provider
IT	Information technology
MAM	Mobile application management
MDM	Mobile device management
MFDA	Mutual Funds Dealer Association
MMS	Multimedia Messaging Service
MTD	Mobile Threat Defense
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
PTR	Pointer
SIN	Social insurance number
SMS	Short Message Service
SPF	Sender policy framework
TCP/UDP	Transmission Control Protocol and User Datagram Protocol
TLS	Transport Layer Security
UEM	Unified endpoint management
VPN	Virtual private network

4.2 Glossary

Term	Definition
Availability	The ability for the right people to access the right information or systems when needed. Availability is applied to information assets, software, and hardware (infrastructure and its components). Implied in its definition is that availability includes the protection of assets from unauthorized access and compromise.
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.
Confidentiality	The ability to protect sensitive information from being accessed by unauthorized people.
Crypto malware	Malware that has the intention to encrypt your data and applications. Usually, crypto malware includes a ransom demand to unlock or decrypt your files.
EDR	Endpoint-Detection-and-Response- Goes hand-in-hand with EPP in that it's software that is used on endpoint devices to detect and prevent malicious activity, however, it can go beyond and remediate endpoints to their pre-infection state.
EPP	Electronic-Protection-Platform is a software solution that is used on endpoint devices to detect and prevent malicious activity, file-based malware attacks and the ability to respond to security incidents and alerts, dynamically.
Integrity	The ability to protect information from being modified or deleted unintentionally or when it is not supposed to be. Integrity helps determine that information is what it claims to be. Integrity also applies to business processes, software application logic, hardware, and personnel.
MAM	Software that has the capability to secure, monitor, manage and support the applications installed on a mobile device that has the correct configuration and/or software agent installed. MAM is different from MDM in that it targets the applications running on the device as opposed to the device itself, though often there is overlap.
MDM	Software has the capability to secure, provision, monitor, manage and support mobile devices deployed within a network by controlling and protecting data and configuration settings. However, the capability of different MDM software packages can vary greatly and care should be taken to select the appropriate solution. MDM is similar to MAM with the difference being that MDM targets the device and operating system itself, rather than the details of installed applications.
MTD	Detects real-time on-device application attacks
Personal health information	Includes identifying information about an individual if the information relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family.
Personally identifiable information	Information that allows the identity of an individual to be determined either directly, or indirectly.
Principle of least privilege	The principle of giving an individual only the set of privileges that are essential to performing authorized tasks. This principle limits the damage that can result from the accidental, incorrect, or unauthorized use of an information system.
Risk	The potential that a given threat will compromise IT assets and cause injury.
Sandbox	A security structure for separating collections of applications from one another, such as personal and employer data on a mobile device.

Term	Definition
TLS	A protocol developed to protect the confidentiality, integrity, and availability of Internet communications between server and client applications.
UEM	Similar to an MDM, an UEM can secure, provision, monitor, manage and support devices such as tablets, cell phones, laptops, desktops and more. The difference with a UEM is in that it is meant to be the central management point for all devices, operating systems, and endpoint security.
Vulnerability	A flaw or weakness in the design or implementation of an information system or its environment that could be exploited to adversely affect an organization's assets or operations.

4.3 References

Number	Reference
1	Personal Information Protection and Electronic Documents Act (PIPEDA). https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
2	Privacy Act. https://laws-lois.justice.gc.ca/eng/acts/p-21/index.html
3	Canadian Centre for Cyber Security. *ITSAP.70.002 Security Considerations for Mobile Device Deployments*. June 2020.
4	Canadian Centre for Cyber Security. *ITSM.10.189 Top 10 IT Security Actions to Protect Internet-Connected Networks and Information.* October 2018.
5	Canadian Centre for Cyber Security. *Baseline Cyber Security Controls for Small and Medium Businesses*. February 2020.
6	Canadian Centre for Cyber Security. *ITSP.40.111 Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information*. August 2016.
7	Canadian Centre for Cyber Security. *ITSAP.30.032 Best Practices for Passphrases and Passwords*. September 2019.
8	Canadian Centre for Cyber Security. *ITSAP.10.096 How Updates Secure Your Device*. *March 2021*.
9	Canadian Centre for Cyber Security. *ITSAP.80.009 Protecting Your Organization While Using Wi-Fi.* October 2020.
10	Canadian Centre for Cyber Security. *ITSAP.80.101 Virtual Private Networks*. October 2019.
11	Canadian Centre for Cyber Security. *ITSAP.40.006 Sanitization and Disposal of Electronic Devices*. October 2020.
12	Canadian Centre for Cyber Security. *ITSP.40.006 IT Media Sanitization.* July 2017.
13	Canadian Centre for Cyber Security. *ITSP.80.022 Baseline Security Requirements for Network Security Zones.* February 2021.
14	Canadian Centre for Cyber Security. *ITSG-38 Network Security Zoning – Design Considerations for Placement of Services within Zones*. May 2009.
15	Canadian Centre for Cyber Security. *ITSP.40.065 Implementation Guidance: Email Domain Protection*. April 2020.
16	Privacy Awareness Training. https://learning-apprentissage.cse-cst.gc.ca/course/view.php?id=194#section-0
17	Canadian Centre for Cyber Security. *ITSM.10.093 Top 10 IT Security Actions: #6 Provide Tailored Cyber Security Training.* February 2020.