

October 2016



MANAGEMENT OF MOBILE DEVICES:
ASSESSING THE MOVING TARGET IN B.C.

www.bcauditor.com

CONTENTS

<i>Report highlights</i>	3
<i>Auditor General's comments</i>	4
<i>Summary of recommendations</i>	7
<i>Response from the Office of the Chief Information Officer</i>	8
<i>Background</i>	10
<i>Audit objective and scope</i>	12
<i>Audit conclusion</i>	14
<i>Key findings and recommendations</i>	15

623 Fort Street
Victoria, British Columbia
Canada V8W 1G1
P: 250.419.6100
F: 250.387.1230
www.bcauditor.com

The Honourable Linda Reid
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Madame Speaker:

I have the honour to transmit to the Speaker of the Legislative Assembly of British Columbia the report, *Management of Mobile Devices: Assessing the moving target in B.C.*

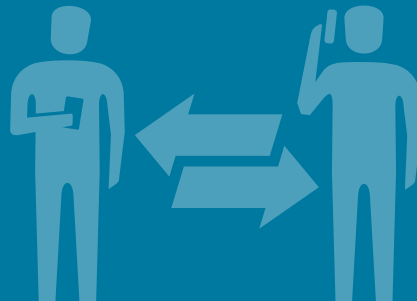
We conducted this audit under the authority of section 11 (8) of the *Auditor General Act* and in accordance with the standards for assurance engagements set out by the Chartered Professional Accountants of Canada (CPA) in the CPA Handbook - Assurance and Value-for-Money Auditing in the Public Sector, Section PS 5400.



Carol Bellringer, FCPA, FCA
Auditor General
Victoria, B.C.
October 2016

REPORT HIGHLIGHTS

Business is
increasingly
conducted with
mobile devices



Mobile devices
can access
SENSITIVE
INFORMATION



CONVENIENCE



often **CLASHES** with



SECURITY

something all
organizations
struggle with

TO PROTECT A DEVICE:

- set a strong password
- set a short inactivity-
until-locked time
- turn on encryption

Government's
mobile device
RISK ASSESSMENT
PROCESS
needs to
improve



Key **security**
settings are
not applied
before devices
go into service

Government has
no central record
of mobile devices

*"You cannot protect
what you don't
know about."*

AUDITOR GENERAL'S COMMENTS

MOBILE DEVICES, SUCH as smartphones and tablets, are an essential part of life. Technology is now sophisticated enough that most, if not all, government business could be done using a mobile device. The convenience of ready access to information is an important benefit, but it comes with increased security risks. Mobile devices are proving challenging to secure.

Mobile devices are subject to many of the same security threats as personal computers (PC) and laptops. But, while PC and laptop security measures have matured over the last decade, many of these measures are only now becoming available on mobile devices.

There are inherent challenges to securing mobile devices. For example, they are incredibly convenient and transportable, but their small size also makes them easy to lose or steal. Also, when new mobile device models become available, the older ones quickly become unsupported and users lose the benefit of regular security updates. And, PCs are usually turned off at the end of each day, but mobile devices often stay connected 24/7, which allows more opportunity for unauthorized access.

In short, maintaining the security of mobile devices requires constant vigilance. Any loss, theft or exposure of sensitive government information – to which these devices have access – could have serious implications for both government and the people of British Columbia. If such a breach were to occur it could also spark a lack of confidence in government's ability to protect the information under its control.

We conducted this audit to determine whether government is managing mobile devices in a manner that maintains the security of sensitive government information. We examined government practices for managing mobile devices. We focused our audit on the role of Office of the Chief Information Officer (OCIO) as it is responsible for leading government's overall strategy and policy on technology. We also examined practices in a sample of five ministries.



CAROL BELLRINGER, FCPA, FCA
Auditor General

AUDITOR GENERAL'S COMMENTS

Technology is constantly changing and government's management of the use of mobile devices needs to keep pace. We found that the OCIO has been proactive in developing a government strategy for mobile device management. However, overall, we found that the OCIO and the selected ministries can do more to improve government's management of mobile devices to ensure that the security of sensitive government information is maintained. Specifically, we found that:

- ◆ there are policy gaps
- ◆ the full life cycle of mobile devices is not well managed
- ◆ appropriate security controls are not always in place
- ◆ there is no central monitoring and logging of mobile device activity

An inventory of all devices that have access to government information is the most critical IT security control. Currently, there is no central record of mobile devices with access to government information. This is concerning because you can't protect what you don't know about.

And, even though government provides security guidance to its employees when they're issued a mobile device, it's left to employees to actually apply some of the settings. As a result, appropriate security settings are not always in place.

For example, inactive devices may be left unlocked for too long, leaving information vulnerable. A short inactivity-until-locked time is by far the most important tool to prevent the unauthorized use of mobile devices. Other key security measures that government leaves to its employees' discretion include: the installation of anti-malware software, regular system and security updates, and more.

AUDITOR GENERAL'S COMMENTS

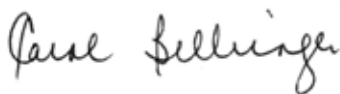
Our report has seven recommendations for government to improve its management of mobile devices, and in particular, improve the security of sensitive government information. Our recommendations include:

- ◆ enhancing policy
- ◆ maintaining an inventory of all mobile devices
- ◆ enforcing security settings
- ◆ monitoring and logging mobile device security incidents
- ◆ analyzing lost and stolen device reports to inform security awareness programs

At the same time we conducted our audit, the [Office of the Information and Privacy Commissioner for British Columbia](#) (OIPC) conducted its own investigation of government's mobile device management. While our audit focused on the security aspects of managing mobile devices, the OIPC's investigation focused on the privacy aspects of mobile device management. Together, our offices have produced a guide to help any resident of B.C. strengthen the security and privacy of both their personal and work devices.

Finally, I am encouraged that government recognizes the risks posed by the rapidly-changing nature of mobile devices. Even before the audit was completed, the Office of the Chief Information Officer was implementing our recommendations to address matters, such as adopting a new mobile device management tool that may be capable of automating the installation and maintenance of anti-malware software, preventing high-risk devices from connecting, and logging security incidents.

I would like to thank everyone we spoke with during our audit for their support, and particularly the OIPC for their partnership.



Carol Bellringer, FCPA, FCA
Auditor General
Victoria, B.C.
October 2016

SUMMARY OF RECOMMENDATIONS

WE RECOMMEND THE OFFICE OF THE CHIEF INFORMATION OFFICER:

- 1** establish requirements to document:
 - ◆ *assessments of the risks associated with new mobile device features and services*
 - ◆ *approvals of risk mitigation plans*
 - ◆ *acceptance of residual risks*
- 2** update the policy framework to clearly identify applicability to mobile devices.
- 3** provide support to help ministries develop a solution to maintain a detailed inventory of all mobile devices (with or without data plans), including key information such as: assignee, manufacturer, model, operating system level and relevant dates.
- 4** ensure all key initial security settings are applied before a mobile device goes into service.
- 5** establish in policy a maximum inactivity-until-locked time based on an assessment of the risks to the security of sensitive government information, and enforce this policy through technical means.
- 6** replace the existing mobile device management tool with one capable of:
 - ◆ *installing and maintaining anti-malware software*
 - ◆ *preventing high-risk devices from connecting*
 - ◆ *monitoring and logging mobile device security incidents*
- 7** analyse lost and stolen device reports for potential enhancements to security awareness programs.

RESPONSE FROM THE OFFICE OF THE CHIEF INFORMATION OFFICER

THE PROVINCE APPRECIATES the careful analysis and valuable recommendations in the Management of Mobile Devices report, recently completed by your office. This timely report has provided valuable feedback to inform our efforts to keep pace with the ever changing and increasing security threats that all organizations face. I appreciate the Office of the Auditor General (OAG) acknowledging the good work we are doing and also in helping to validate government's current course of action to increase security in the area of mobile devices. The Province accepts all 7 recommendations in the report.

The protection of government and citizen information is of primary importance. While government has security controls to protect all mobile devices and the information residing on them there is more we can do in this area. Existing controls include password protection, device encryption, ability to remotely wipe a device that is lost or stolen, and the ability to automatically lock a device that is inactive for a period of time.

The Office of the Chief Information Officer executed its plan to roll out the new Mobile Device Management Service (MDMS) in July, 2016. All 12,000 mobile devices will be protected by the MDMS by December 31, 2016. The introduction of this new service will enable government to meet 4 of the 7 OAG recommendations, including:

- ◆ provide ministries the ability to maintain a detailed inventory of all mobile devices
- ◆ ensure additional security settings are applied before a mobile device goes into service

- ◆ enforce a maximum inactivity-until-locked time through technical means
- ◆ replace the existing mobile device management tool with one capable of
 - ◆ installing and maintaining anti-malware software
 - ◆ preventing unauthorized mobile devices from connecting
 - ◆ monitoring and logging mobile device security incidents

To address the remaining 3 recommendations, the Province will amend existing policies to explicitly apply to mobile devices, and will formalise its documented processes for:

- ◆ assessment of risks associated with new mobile device features and services
- ◆ approval of mitigation plans and acceptance of residual risk

RESPONSE FROM THE OFFICE OF THE CHIEF INFORMATION OFFICER

- ◆ analysis of lost and stolen device reports for enhancements to security awareness programs

These policy and process improvements will be completed by March 31, 2017.

The Province accepts the valuable recommendations of the Office of the Auditor General which will improve the government device strategy, the information security program, and the protection of personal information.

Bette-Jo Hughes
Associate Deputy Minister and
Government Chief Information Officer

BACKGROUND

PRIVATE AND PUBLIC organizations have been providing their employees with mobile phones for a number of years. But, recently there have been two significant developments:

- ◆ mobile devices have evolved far beyond their original telephone and email capability
- ◆ BlackBerry® devices, once the *de facto* standard, are being replaced by rapidly evolving devices that have more features

We are now at the point where most business could be done using mobile devices — smartphones and tablets — instead of traditional computers. And BlackBerry® devices, known as secure and controlled, are now outnumbered by devices with greater flexibility and range of features.

Manufacturers continually boost device performance, adding convenience and productivity features, which drive employee demand for the latest mobile devices. But, the newer devices are more difficult to manage, and manufacturers have been slow to add security features like those on traditional computers.

Governments, along with most other organizations, are finding management of mobile devices challenging. Some of the challenges arise because a device's strength can also be a weakness: Small size?

That means the device is easily lost or stolen. Always on/always connected? That means hackers have more opportunities to break in.

Other challenges arise from factors unique to mobile devices:

- ◆ there is a tendency to use simple passwords due to the lack of a physical keyboard
- ◆ frequent model changes mean devices quickly become unsupported (can't get security updates)
- ◆ evolving operating systems provide opportunities for malware (malicious software)
- ◆ mobile device apps often demand more access to sensitive information, like contacts or location information

When mobile devices that have access to sensitive government information are not well-managed or secured, there is a higher likelihood of:

- ◆ exposure of confidential information of the people of B.C.
- ◆ economic harm to government through loss of intellectual property or competitive advantage
- ◆ loss of confidence in the ability of the government to protect information it has collected

LOSS & THEFT

Studies show that:

- ◆ one in 10 smartphone users have had their phones stolen
- ◆ for lost-but-returned devices, more than 90% of the good Samaritans snooped before returning them

BACKGROUND

In the B.C. government, the Office of the Chief Information Officer (OCIO) leads strategy, policy and standards for telecommunications, information technology, IT security and the management of the IM/IT investment portfolio for ministries. The OCIO is accountable for the strategic direction of IT across government, and deputy ministers are accountable for ensuring that their ministries adhere to the OCIO's IT governance directions.

The policy framework that applies to mobile devices includes Chapter 12 of the *Core Policy and Procedures Manual (CPPM) - Information Management and Information Technology*, and the OCIO's *Information Security Policy (ISP)*. Ministries are mandated to comply with those policies in their own management of computing activities. Periodically, the OCIO publishes guidance to supplement the two policies for clarity and direction.

AUDIT OBJECTIVE AND SCOPE

AUDIT OBJECTIVE

We conducted this audit to determine whether the Government of British Columbia is managing the use of mobile devices in a manner that maintains the security of sensitive government information.

Specifically, we examined whether:

- ◆ government has proactively protected sensitive government information through mobile device technology planning and policy development
- ◆ the full lifecycle of mobile devices is managed in a manner that minimizes the risk of sensitive government information being accidentally exposed or stolen
- ◆ appropriate security controls are in place to protect sensitive government information that is accessed, stored or transmitted by mobile devices
- ◆ mobile device activity is monitored and logged, and security incidents are responded to in a manner that protects sensitive government information

SCOPE

We examined government practices for managing mobile devices by focussing on the OCIO and a sample of five ministries. We chose the ministries based on a combination of three factors: (a) those with the highest reported numbers of lost and stolen devices, (b) those expected to have the highest remediation cost if a data breach were to occur, and (c) those where privacy risks were expected to be highest.

The ministries sampled were:

- ◆ Ministry of Children and Family Development
- ◆ Ministry of Finance
- ◆ Ministry of Forests, Lands and Natural Resource Operations
- ◆ Ministry of Justice
- ◆ Ministry of Health

We carried out our audit work between June and November 2015.

We examined government's mobile devices that have access to internal government services and data. We included smartphones, tablets and other devices running mobile-specific operating systems (e.g., Android, Blackberry, iOS). Our audit included a review of policy and guidance, interviews with OCIO and ministry staff and analysis of government records related to mobile devices.

Public bodies and Crown agencies were excluded from the scope of this audit.

AUDIT OBJECTIVE AND SCOPE

APPROACH

Because security and privacy are strongly linked, our office and the Office of the Information and Privacy Commissioner (OIPC) agreed to conduct concurrent examinations of government's management of mobile devices.

The OIPC focussed on the privacy policy aspects of managing mobile devices, whereas our office focused on the security aspects of managing mobile devices. The OIPC report is available on their website.

Our audit objectives and criteria were based on international information security frameworks and standards including: COBIT (Control Objectives for Information and Related Technologies), and those of the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST).

We conducted the audit in accordance with the standards for assurance engagements set out by the Chartered Professional Accountants of Canada (CPA) in the CPA Handbook — Assurance and Value-for-Money Auditing in the Public Sector, Section PS 5400, and under the authority of Section 11 (8) of the *Auditor General Act*.

AUDIT CONCLUSION

Technology is constantly changing and government's management of the use of mobile devices needs to keep pace. Overall, we found that the OCIO and select ministries can do more to improve government's management of mobile devices in a manner that maintains the security of sensitive government information. Specifically, we found that:

1. the OCIO has been proactive in developing a strategy for mobile device management, but needs to address some gaps in policy
2. the full mobile device lifecycle is not well managed; in particular, there is no central inventory of mobile devices for government
3. appropriate security controls are not always in place; in particular, inactive devices are left unlocked too long
4. mobile device activity is not being monitored or logged, but security incidents are managed well for reported cases of loss and theft

KEY FINDINGS AND RECOMMENDATIONS

GOVERNMENT HAS DEVELOPED MOBILE DEVICE STRATEGIES

Government recognizes that the fast-moving technology of mobile devices comes with risk. Convenience and productivity-enhancing features and services — introduced with each new mobile device and software update — create risks to the security of sensitive information. If the risks are not assessed before new device features or services are implemented, sensitive information could be exposed, altered or destroyed

As a result of these evolving threats, the Office of the Chief Information Officer (OCIO) has prepared several *mobile device strategy* papers: the first was issued in late 2013 and the second in early 2015. Both papers discuss strategic topics, including procurement, deployment and security. Government plans to implement these strategies over the next three years.

One strategy government identified was the need for an effective mobile device management tool. In response, the OCIO prepared a document introducing its *Enterprise Mobility Management (EMM) Proof of Concept* project. The project is intended to assess a new mobile device management tool and its ability to “effectively and securely manage devices and mobile applications.”

MOBILE DEVICE RISK ASSESSMENT PROCESS INSUFFICIENT

Because of the evolving threats inherent in mobile devices, we expected the OCIO to have established a formal process for continuously monitoring and assessing the risk of technological changes before adopting them into the workplace. However, we found that the assessment process for mobile device features and services is not sufficiently robust.

At the time of our audit, the OCIO had two groups of employees responsible for examining new mobile devices and mobile device-related services for possible risks to sensitive information. Staff in one group performed monitoring of risks from emerging mobile device features and services. The other group assessed device technical capabilities — some of which were security related. After the assessments, the OCIO used email and internal government website posts to inform ministry employees which devices and services were approved for use. We noted that both groups are experienced and knowledgeable. However, we observed that the groups did not:

- ♦ formally define or document mobile device risk assessment processes
- ♦ have evidence that senior management reviewed and approved all risk assessments for mobile devices or that risk mitigation plans were derived from risk assessments

KEY FINDINGS AND RECOMMENDATIONS

- ◆ identify, assess or acknowledge residual risks (risks that remain after management has applied security controls)

RECOMMENDATION 1:

We recommend that the OICO establish requirements to document:

- ◆ *assessments of the risks associated with new mobile device features and services*
- ◆ *approvals of risk mitigation plans*
- ◆ *acceptance of residual risks*

MOBILE DEVICE POLICIES UNCLEAR

The OCIO has established several policies and guidance documents governing the use of computing resources and security. Chapter 12 of government's *Core Policy and Procedures Manual (CPPM)* provides policies on *Information Management and Information Technology* and the OCIO's *Information Security Policy (ISP)* covers computing security.

We reviewed version 2.2 of the ISP (last updated in 2012) and Chapter 12 of the CPPM. We expected, but did not find, policies addressing risks associated with the following:

- ◆ bring your own device (BYOD) programs
- ◆ modifications to the operating system software and security settings
- ◆ installation of applications from unreliable sources
- ◆ the large range of application sources

We recognize that certain generic security policies can be extended to include mobile devices — such as the requirement that threat/risk assessments be done for devices that contain sensitive information — but applicability of many policies is open to interpretation.

The OCIO has published several *Policy Summary Guidance* documents. These documents are supplemental to the policies they are designed to clarify. They can be used as guidance by government employees motivated to manage the risks of mobile computing. Ministries have also developed their own guidance on the use of mobile devices by ministry staff and, in some cases, by contractors. We reviewed these guidance documents and found that they addressed the majority of mobile computing risks.

We also reviewed government's *Appropriate Use Policy* and noted that it is not clear whether personal mobile devices are allowed or disallowed for work. And even then, there are inconsistencies between the ministry-developed guidance and the core policies of the government; one of the five ministries we examined allows contractors to use their own devices for conducting government business. However, the OCIO stated that BYOD is not allowed.

RECOMMENDATION 2: *We recommend the Office of the Chief Information Officer update the policy framework to clearly identify applicability to mobile devices.*

KEY FINDINGS AND RECOMMENDATIONS

MOBILE DEVICE LIFECYCLE NOT MANAGED

Inventory

The most critical security control for computing environments is an accurate and up-to-date inventory of technology assets. This includes hardware, software and network infrastructure. The importance of an inventory is embodied in the information security tenet “*You cannot protect what you don’t know about.*” We observed that ministries do not have an effective way to verify the accuracy and completeness of their mobile device inventory.

INVENTORY IS #1

The respected Centre for Internet Security [lists Inventory of Authorized and Unauthorized Devices](#) as the most critical IT control

When unknown devices are connected to corporate resources there is a greater chance that vulnerabilities in the device’s hardware or software can provide unauthorized access to sensitive information. Therefore, it is critical that only authorized devices with authorized software be allowed to connect to the organization’s computing resources.

Government’s CPPM states that ministries are responsible for the administration, control, proper accounting and safeguards of their devices. Therefore, we expected ministries to have established effective asset management systems for tracking ministry-owned or ministry-controlled mobile devices.

Of the five ministries we reviewed, the practice of tracking mobile devices assets varied. We found:

- ♦ there is no central record of mobile devices owned or controlled by the ministries
- ♦ tracking of mobile devices was decentralized and done at a branch or business unit level
- ♦ periodic reviews for accuracy of the information tracked was ad hoc
- ♦ mobile devices without data plans were not tracked
- ♦ some key information, such as assignees, operating system software versions, applications installed, was missing

Government uses a mobile device management tool, centrally administered by the OCIO, to manage the connectivity of mobile devices to government systems. Requests to connect a device are made by ministries via an online ordering system. Requests are received by the OCIO and an account is setup in the mobile device management tool for the person using the mobile devices.

We expected that an inventory of mobile devices could be determined from the information tracked in both the *mobile device management tool* and the *online ordering system*. However, this was not possible as there are no consistent data fields to link the two sources. In addition, we noted that once an account is created in the mobile device management tool, multiple devices can be connected without corresponding online orders.

KEY FINDINGS AND RECOMMENDATIONS

Security settings

For optimal protection of sensitive information, some key security settings need to be applied *before* a mobile device goes into service. These settings include: encrypting the device's storage, setting an initial inactivity-until-locked time and installing anti-malware software.

We found that government employees are provided some guidance on these key settings. However, the work of applying security settings to a device requires a technical mindset and there is a risk that even skilled and motivated users may not notice the guidance documents left to their responsibility.

Additionally, in some circumstances, contractors are permitted to use non-government mobile devices to carry out government business. One of the terms in the standard government contract is that the contractor must protect personal information by making reasonable security arrangements. We noted that one of the five ministries provides guidance on what those security measures are. However, once again, the onus of applying the security measures rests with the user.

RECOMMENDATION 3: *We recommend the Office of the Chief Information Officer provide support to help ministries develop a solution to maintain a detailed inventory of all mobile devices (with or without data plans), including key information such as: assignee, manufacturer, model, operating system level and relevant dates.*

RECOMMENDATION 4: *We recommend the Office of the Chief Information Officer ensure all key initial security settings are applied before a mobile device goes into service.*

MOBILE DEVICES UNLOCKED TOO LONG WHEN INACTIVE

Mobile device encryption has made news headlines a number of times this year and rightly so. Encryption reduces the likelihood that unauthorized individuals – even those well-equipped and determined – can access sensitive data from a device.

We reviewed government's encryption settings and found that they are consistent with good practice in preventing unauthorized access to sensitive information. We found that government applied encryption not just to the mobile devices, but also to removable media (e.g., memory cards) on the devices.

All modern mobile devices provide users with the ability to set an inactivity-until-locked time that will cause their screens lock after a period of inactivity. When a device's screen is unlocked, other protection measures, including encryption, are completely bypassed. So although encryption provides strong protection from unauthorized access, it is supplemental to the sophistication of the password setting and the inactivity-until-locked time.

We reviewed the password settings used by government and found that they are consistent with good practice in preventing unauthorized access.

During our fieldwork, we found that the inactivity-until-locked time was set to 60 minutes by the OCIO's mobile device management tool. This inactivity-until-locked time is significantly higher than the OCIO's own guidelines of no more than 15 minutes. When we brought this to the attention of OCIO staff, they quickly changed the default to 15 minutes. This

KEY FINDINGS AND RECOMMENDATIONS

discrepancy was likely the result of an oversight. Users could have further reduced the time on a device-by-device basis, but they were likely unaware of the feature.

After choosing a password, a short inactivity-until-locked time is by far the most important control to prevent unauthorized use of a mobile device.

The longer the screen remains unlocked the higher the risk that someone other than the device owner may, through possession alone, have unauthorized access to sensitive information available to the device. Therefore, after choosing a password, a short inactivity-until-locked time is by far the most important control to prevent unauthorized use of a mobile device.

RECOMMENDATION 5: *We recommend that the Office of the Chief Information Officer establish in policy a maximum inactivity-until-locked time based on an assessment of the risks to the security of sensitive government information, and enforce this policy through technical means.*

LIMITATIONS TO GOVERNMENT'S MOBILE DEVICE MANAGEMENT TOOL

Malware

Mobile devices can be infected with malware (malicious software) just like desktop or laptop computers can. Information on any malware-infected device is at risk of:

- ◆ undetectable, long-term viewing (spying) by unauthorized individuals
- ◆ unauthorized alteration, deletion or lock-out

MALWARE RISING

New mobile malware tripled in 2015. Growth continues in 2016 with ransomware (which blocks access until a user pays a sum of money) as the latest flavour.

Unlike traditional computers, mobile devices rarely have built-in anti-malware capability. Where it is not built-in, third party anti-malware software will need to be installed where appropriate.

We found that government leaves the responsibility of installing anti-malware software to the employees who use the mobile devices, rather than to technical

KEY FINDINGS AND RECOMMENDATIONS

support staff. The OCIO's current mobile device management tool is incapable of automating the installation of anti-malware software. Additionally, it cannot detect whether or not the user has installed anti-malware software.

Unpatched/unsupported devices

Mobile devices require timely operating system updates, or patches, to stay secure just as desktops and laptops do. For traditional computers, once the software maker has developed a patch, it is usually delivered, and even installed, automatically. This is in sharp contrast to some mobile device patches which can involve each of: the software maker, the hardware manufacturer (if different), the mobile phone service provider and, finally, the device user. Any one of the additional players in a mobile device patching sequence can delay or block the installation.

Worldwide, the situation of unpatched devices is particularly acute with Android devices. As of this writing, 30% of devices in use are *unsupported* by manufacturers, meaning they are out-of-date and will never be patched.

Modified devices

Some users modify their mobile device's operating system — a process known as jailbreaking (Apple iOS) or rooting (Android). Motivations to make the modification usually include one or more of the following: to add features to the device, to have greater

freedom choosing applications (unless modified, most devices are limited to official app stores) or to bypass security settings made by government.

When a user modifies the operating system of a mobile device, there is an increased risk that:

- ◆ the user may now be able to disable security features
- ◆ the modified device will be more susceptible to malware (malicious software) which similarly jeopardizes the security of the information
- ◆ the device immediately becomes infected (some rooting or jail-breaking processes involve the installation of infected operating systems at the outset)
- ◆ the device will no longer receive security updates, or patches, from the manufacturers and will therefore stay vulnerable

We expected government to have controls in place to prevent or block unsecured devices from connecting to and accessing sensitive information. We found that the current mobile device management tool was not able to:

- ◆ keep operating systems and apps up-to-date
- ◆ block devices with operating systems that are no longer supported by the vendors
- ◆ install or require anti-malware software on devices which connect to it
- ◆ stop modified (jail-broken or rooted) devices from connecting

KEY FINDINGS AND RECOMMENDATIONS

SECURITY INCIDENT MONITORING/ LOGGING CAPABILITIES MISSING

Incident monitoring & logging

Monitoring and logging are key controls to detect and prevent security incidents that threaten information resources. Therefore, we expected government to have established these controls for mobile devices.

We found that the OCIO's current tool lacks the capability of monitoring or logging mobile device security incidents. As noted earlier, incidents such as malware outbreaks or the connection of unauthorized devices are beyond the capabilities of the OCIO's current mobile device management tool.

Preventing incidents is preferable to detection. However, as prevention can never be 100% effective, well-managed organizations use some combination of incident prevention and incident detection.

The sheer number of security incidents an organization faces mean incident detection and incident prevention should be automated as much as possible. Incident handling technology can provide reports, watch for trends and then communicate when the incidents require human intervention. During our audit, the OCIO was handling mobile device incidents using its mobile device management tool. The tool can do some incident prevention, but it is extremely limited in capability. For example, it cannot prevent a jailbroken/rooted device from connecting or detect one after it has connected.

RECOMMENDATION 6: We recommend that the Office of the Chief Information Officer replace the existing mobile device management tool with one capable of:

- ♦ installing and maintaining anti-malware software
- ♦ preventing high-risk devices from connecting
- ♦ monitoring and logging mobile device security incidents

REPORTS OF LOST/ STOLEN DEVICES ARE DELAYED

Incident response

Because the OCIO's current tool lacks incident monitoring and logging capability, the only type of incident response we could examine were cases of reported device loss and theft.

We found there are central incident reporting, identification and recording processes. We also found evidence that the OCIO and ministries respond to reported cases of mobile device loss and theft in a way that protects sensitive information.

The OCIO has the capability of remotely wiping (erasing) a mobile device's storage. And we found evidence that this capability is used when devices are reported lost or stolen. However, it's important to note that remote wipe is a limited control: it assumes the device was not already accessed before the screen locked and the device must be on and able to receive

KEY FINDINGS AND RECOMMENDATIONS

a network signal for the control to work. Also, the OCIO has no way to know whether the remote wipe was successful because confirmation is not guaranteed.

Most significantly, we found extensive delays — on average 2-6 days, but in some instances, as long as 60 days — between when a device was lost and when it was reported missing by the employee. This prevented government from taking prompt action to mitigate the risk of information exposure.

Also, at one ministry, employees were advised not to report lost devices for up to three days in case the device could be found.

RECOMMENDATION 7: *We recommend that Office of the Chief Information Officer analyse lost and stolen device reports for potential enhancements to security awareness programs.*



OFFICE OF THE
Auditor General
of British Columbia

Location

623 Fort Street
Victoria, British Columbia
Canada V8W 1G1

Office Hours

Monday to Friday
8:30 am – 4:30 pm

Telephone: 250-419-6100

Toll free through Enquiry BC at: 1-800-663-7867

In Vancouver dial: 604-660-2421

Fax: 250-387-1230

Email: bcauditor@bcauditor.com

Website: www.bcauditor.com

This report and others are available at our website, which also contains further information about the Office.

Reproducing

Information presented here is the intellectual property of the Auditor General of British Columbia and is copyright protected in right of the Crown. We invite readers to reproduce any material, asking only that they credit our Office with authorship when any information, results or recommendations are used.



AUDIT TEAM

Sheila Dodds
Assistant Auditor General

David Lau
Director, IT Audit

John Bullock
Senior IT Audit Specialist

Stan Andersen
Manager, IT Audit



OFFICE OF THE
Auditor General
of British Columbia