BlackBerry

White Paper

# A Mobile Security Checklist: The Top Ten Threats to Your Enterprise Today

As enterprises mobilize business processes, more and more sensitive data passes through and resides on mobile devices. And while almost every CIO knows how important mobile security is, getting a grip on it can be tough. There's a lot to consider, and new factors enter the equation all the time. On the pages that follow, you'll find an overview of the key issues you need to be on top of right now to protect your organization, its employees and its customers. If you answer no to many of these questions, you may have some significant gaps in your approach to mobile security.

The good news is that you're not alone – and there are endpoint security and management solutions designed to address each of these challenges.

## The Top 10 Enterprise Mobility Security Threats Today

1. Inadequate control over lost/stolen devices
2. Poor security for IP leaving your network
3. Users who don't follow mobile policies
4. Rogue apps and malware
5. Poor separation of work and personal content and apps
6. Limited protection for data at rest and in transit
7. Weak authentication
8. Difficulty monitoring & managing the entire mobile fleet
9. Challenges with compliance and flexibility (meeting the needs of all users)
10. Inconsistent security due to OS fragmentation

## 1 Do you stay in control when devices go missing?

- Are your procedures for lost/stolen devices clearly defined, well understood by your entire staff and adhered to?
- Is IT able to perform a remote wipe (and confirm that data is permanently deleted)?
- Do you impose password protection on every device, regardless of who owns it? (Bring Your Own Device; Corporate Owned, Personally Enabled; etc.)?
- Do you insist that devices automatically lock after a defined period of inactivity?
- Are the devices in your network (again, regardless of the ownership model) discoverable via location-based tracking?
- Do you have backup and restore capabilities that allow you to provision a new device quickly and easily?
- Can mobile workers and safely initiate some remote security tasks themselves through a user self-service tool (e.g. locking a misplaced device remotely)?

## 2 Are you taking measures to protect your documents, as well as your devices?

- Does your IT department have a means of controlling files when they leave the firewall?
- Do you have protections in place against screen captures and unauthorized printing/downloads?
- Does your enterprise use an enterprise file sync and share (EFSS) solution?
- Do you protect your outgoing email attachments?
- Can you enable content/file sharing securely?

## 3 Do your users understand and follow your policies?

- Are your employees aware of how social engineering works, and how to protect themselves against it?
- Do employees understand the risk of using unsecured, third-party applications in the workplace?
- Do you provide training and documentation for new employees that explains how they should approach mobile computing?
- Is that training reinforced regularly and in different ways?
- Do employees truly understand what's expected and why it matters?
- Do you account for different learning styles (some users will respond better to video; others to a checklist, etc.)?
- Do you ask users to sign your policy document and are they aware of the penalties for not complying?

## 4 How do you keep rogue apps and malware at bay?

- Do all devices accessing your network have appropriate anti-virus/anti-malware capabilities installed or built-in?
- Do you keep an up-to-date whitelist of third-party apps?
- Can you run a quick check at any time to make sure that all the apps in use are authorized?
- Are BYOD users required to keep devices current with OS upgrades, software and app updates, and (if not built-in) anti-virus protection?
- Do you have a corporate app storefront?
- Do you have a means of enabling developers to quickly deploy secure corporate apps?
- Do you have a mechanism in place to manage apps throughout their lifecycle (deployment, updates, retirement)?
- Are you able to automatically detect when jailbroken or rooted devices try to access your network and can you automatically program next steps?
- Can employees find out which apps are approved, recommended or mandatory for their role?
- Are users prompted to enter their device password before installing apps?
- Are your anti-virus measures for non-mobile devices up to date and adequate? (Malware exposure can occur when users connect a mobile device to an infected desktop computer via USB, but most desktop anti-virus software will help prevent this type of attack.)
- Do you protect your corporate applications from malicious software through containerization/sandboxing?
- Are interactions between your applications secured/encrypted?

## 5 How do you keep work and personal content/data separate?

- Can you enable and control a separate work space or container on the devices you manage, across multiple operating systems?
- If you use tools like location-tracking applications, are they disabled outside the work profile?
- Do you have a mechanism to prevent data leakage across multiple devices (e.g. making it difficult for users to send corporate data through unsecure channels like social media)?

## 6 Can you ensure data is secure, at rest and in transit?

- Can you enforce encryption for data that's resting on devices and for data in transit to the standard your policies demand?
- Are users prevented from disabling encryption manually?
- Can app data move securely along its path without a third-party VPN?
- Do you have confidence that your systems can protect your customers' data regardless of how closely employees follow your policies?
- Are you protecting your network against external threats, like unsecure business partners?

## 7 How do you control authentication?

- Do you authenticate devices and users beyond single-factor identification?
- Do your systems produce an alarm when an unauthorized device accesses the network? Can you control what happens next?
- Have you tested your authentication processes for vulnerabilities?
- Have you enabled single sign-on for SaaS/cloud applications?
- Are you able to seamlessly manage users with multiple registered devices?

## 8 Can you monitor your mobile ecosystem in real-time?

- Are you able to get a quick snapshot of your complete mobility landscape, through a unified dashboard?
- Can you easily create and export reports for auditing/compliance/logging?
- Can you configure your systems to create alerts and take automatic actions when security breaches are detected?
- Do you have full visibility into how and where devices in your fleet are being used at any given time?

## 9 Can you apply appropriate security policies to the various user profiles in your organization?

- Are you able to provide the highest security for those users who require it?
- Do your users have to sacrifice convenience for the sake of security?
- Are you able to meet all the compliance requirements of your industry?

10

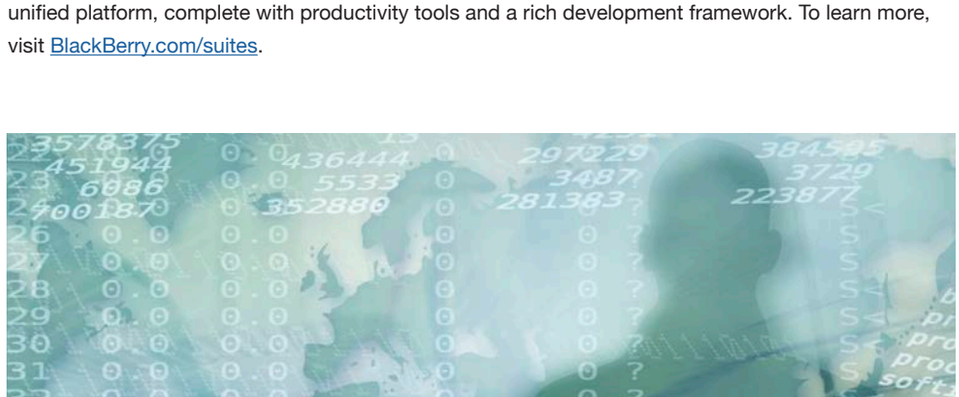
## Are you able to deal with device fragmentation?

- Do you know which specific devices are being used within your organization?
- Are users provided with a wide range of choices in terms of mobility? What tools do you use to help ensure that BYOD users are upgrading their operating systems as soon as patches and updates are available?
- For users with multiple mobile devices, are you using Identity and Access Management tools for more efficient authentication?
- Are your security solutions device-agnostic, and consistent across your mobile fleet?

## How to protect your organization

The BlackBerry platform is purpose-built for security, to deliver the best protection for work content, at rest and in transit, across the operating systems that matter, including iOS, Android™, Windows® Phone and BlackBerry.

And now, with the Good Secure EMM Suites, we're better-equipped than ever to provide you with a comprehensive EMM platform that's suited for every corporate use case. Designed for flexibility, the Secure EMM Suites seamlessly integrate document control, MDM, MAM, and MCM into a single, unified platform, complete with productivity tools and a rich development framework. To learn more, visit BlackBerry.com/suites.




## About BlackBerry

BlackBerry is securing a connected world, delivering innovative solutions across the entire mobile ecosystem and beyond. We secure the world's most sensitive data across all end points – from cars to smartphones – making the mobile-first enterprise vision a reality. Founded in 1984 and based in Waterloo, Ontario, BlackBerry operates offices in North America, Europe, Middle East and Africa, Asia Pacific and Latin America. The Company trades under the ticker symbols "BB" on the Toronto Stock Exchange and "BBRY" on the NASDAQ. For more information, visit www.blackberry.com.