THE TOP 8 MOBILE SECURITY RISKS

How to Protect Your Organization

Whitepaper

SERIOUS MOBILITY FOR SERIOUS BUSINESS

BlackBerry | ENTERPRISE

The Top 8 Mobile Security Risks: How to Protect Your Organization

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 EMM solutions designed to address each of these challenges.

The Top 8 Enterprise Mobility Security Issues Today

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

1. Do you stay in control when devices go missing?	Yes	No	I'm not sure
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 brief 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 easily and safely initiate some remote security tasks themselves through a user self-service tool (e.g. locking a misplaced device remotely)?			

2. Do your users understand and follow your policies?	Yes	No	I'm not sure
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 they 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 of not complying?			

3. How do you keep rogue apps and malware at bay?	Yes	No	I'm not sure
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 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.)			

4. How do you keep work and personal content/data separate?	Yes	No	I'm not sure
Can you enable and control a separate work space or container on the devices you manage, across multiple operating systems?			
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)?			
Can you enable content/file sharing securely? Can mobile users securely view, edit, and share files, and save them securely for offline use?			

5. Can you ensure data is secure, at rest and in transit?	Yes	No	I'm not sure
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?			

6. How do you control authentication?	Yes	No	I'm not sure
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?			

7. Can you monitor your mobile ecosystem in real-time?	Yes	No	I'm not sure
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?			

8. Can you apply appropriate security policies to the various user profiles in your organization?	Yes	No	I'm not sure
Are you able to provide the highest security for those users who require it?			
Are you able to meet all the compliance requirements of your industry?			

How to protect your organization

If you're looking for answers to any of the challenges in this checklist, think BlackBerry®.

The BlackBerry platform is purpose-built for security, to deliver the best protection for work content, on device and in transit, for corporate, COPE and BYOD devices – whether they're running iOS, Android™, Windows® Phone or BlackBerry operating systems.

Work email, content and apps are seamlessly separated from personal email, content and apps, with no compromise to the user experience. The BlackBerry security model delivers fast, multi-platform app deployment, and fully encrypted, behind-the-firewall content access without the need for third-party VPNs or add-on security. A user self-service portal allows for simple security management. And optional Gold level EMM provides the highest security control, enabling full compliance for government, high-security and regulated environments.

To find out more and to sign up for a free 60-day BES12 trial, head to **blackberry.com/enterprise** [1]

[1] 60-day Free Trial Offer: Limited time offer; subject to change. Limit 1 per customer. Trial starts upon activation and is limited to 50 Gold BlackBerry subscriptions and 50 Secure Work Space for iOS and Android subscriptions. Following trial, customer must purchase subscriptions to continue use of product. Not available in all countries. Subscriptions can be purchased direct or from authorized resellers. When a system is upgraded to production, the trial subscriptions will no longer be available. This Offer is void where prohibited and is subject to modification, extension or early termination at BlackBerry's sole discretion.