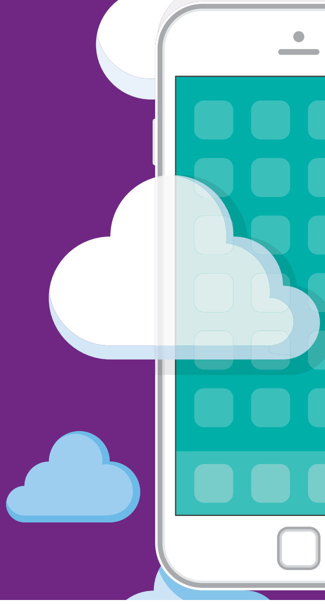
KPMG

10 key mobile risks

Enterprise user's perspective



What we do:

KPMG LLP's (KPMG) Emerging Technology Risk Mobility Services practice comprises an experienced, cross-functional team possessing the industry, regulatory, and functional knowledge, as well as the requisite technical skills, to help assess, design, and implement risk-mitigating approaches for your mobile-enabled enterprise. We help our clients by performing mobile device security and governance assessments, mobile application assessments, and mobile strategy and operating model reviews in line with the key issues currently facing your industry. We leverage our internally developed Mobile Device Security and Governance (MDSG) toolkit and KPMG Enterprise Mobility Framework (KEMF) to help our clients establish mobile programs that strike the right balance between usability and security in the short-term as well as develop sustainable strategies to match enterprise mobility growth in the long-term.

10 key mobile risks:

The mobile landscape continues to evolve. With increasing user adoption rates, the multitude and magnitude of risks that consumers and business enterprises face on a daily basis is rising. According to Statista, "The overall number of mobile phone users reached 4.43 billion in 2015. This number is expected to grow to 4.61 billion in 2016 and 4.77 billion in 2017." For the enterprise workforce, awareness is the first step to mitigating these risks and helping ensure data security and privacy are maintained. For business enterprises, selection of a suitable and secure technology platform (i.e., mobile device management [MDM] tools or similar solutions) is integral to effective management and monitoring on an ongoing basis. Business enterprises should not simply set policies within their mobile solution and expect results — constant monitoring is necessary to meet business and technology goals. Protecting the enterprise against compromised mobile devices with access to sensitive data can only be accomplished with processes supported by adequate technology. An understanding of the mobile environment, along with the potential attack surfaces a hacker can exploit, is necessary to respond to the security and privacy risks that are both known and continually evolving. Mobile hardware and software vendors attempt to stay up-to-date with releases to address new and existing mobile risks, but a strong mobile program and user awareness is paramount to protect against these threats. Let us look at some of the most common and pervasive risks that exist and explore simple ways users can minimize or mitigate them:

1. **Wi-Fi risks**
   Users should avoid connecting to public or unknown Wi-Fi hotspots. These access points are often insecure and may be easily spoofed, which is a way for an attacker to inappropriately access a device without user awareness. Also, users should be careful about saving Wi-Fi connections to these access points (such as hotel Internet, coffee shops, etc.) as these saved connections can be collected and an automatic connection to a spoofed access point could be started to obtain data.

2. **Text message entry point**
   SMS and MMS are some of the primary methods for device compromise. Users should not open and delete text messages which appear suspicious or those not from known numbers or contacts. These messages could install malware or compromise device security.

3. **Lost or stolen devices**
   Users should fully understand that lost or stolen devices containing sensitive information should be reported immediately. This is important to protect both company information and their personal information. Additionally, users should be fully informed of the tools available to protect devices, such as "Find my Phone", remote lock, and wipe tools, among others.

4. **Sensitive data stored in contacts or notes**
   Users should avoid storing sensitive information (such as passwords) in locations not intended for these purposes. For instance, information stored within a user's contacts may be accessed by apps which are granted this access. Sensitive information should only be stored in approved and secure containerized apps.

5. **Beware cloud sync**
   Automatic synchronization of mobile device data to a cloud service (Apple iCloud®, Dropbox, etc.) should configure these services to sync only approved and/or appropriate information. For example, if photos containing sensitive information are stored on the device, these should be deselected from automatic synchronization. If sensitive information is approved for upload, it should be only to approved solutions with appropriate security and access controls.

6. Approved App Store download

Users should only obtain mobile apps from approved app stores, such as Apple iTunes®, Google Play, and their organization's enterprise app store. Apps obtained from other sources may not be subject to the same level of review and controls to prevent malware and could compromise a device's functions or data.

7. Unencrypted app data

Unencrypted data in messaging applications such as WhatsApp (location data) and Viber (photos, videos, and location images) may be made available to hackers despite the applications being marketed as encrypted. Oftentimes, the data is not stored on the application's server in an encrypted manner, meaning that if a hacker had knowledge of a message URL, it could retrieve the data from the application server and do whatever it would like with it.

8. Counterfeit apps

Unauthorized, or "rogue" apps, as they have come to be called, may contain viruses, malware, or other types of malicious code. When installed on a mobile device, these apps can steal data, including contact lists, bank account numbers, medical records, or potentially anything else stored on the device. Users should never download an application without looking into the developer behind it or being aware of app permissions, such as requesting access to personal information or files that are not serving the app's intended purpose.

9. Rogue device connections

Users should be aware of potential rogue devices when making network connections in public places. Rogue devices can give away seemingly free and safe Internet, Bluetooth, or near-field communication (NFC) connections that, in fact, are vulnerable to unauthorized access attempts. These attackers are looking for passwords, corporate gateways, other useful information to infiltrate a company's network, or sensitive data. This is often referred to as a "man in the middle" attack.

10. Device sharing

If the user's device has sensitive information stored or access to sensitive information, use discretion while sharing with others. On iOS, a specific form of device sharing — AirDrop® connection — could result in the installation of malware. If AirDrop is turned on for the user's mobile device, a hacker can silently install malware on Apple's Springboard software even if the file is rejected. This type of attack would give the hacker access to the device's contacts, camera, location, and more.

Solutions and call to action:

Current solutions fall short of fully addressing the ever-changing face of mobile risks. At both the workforce and business enterprise level, users often do not treat mobile devices with the same level of security as they would a laptop. However, both act as gateways to the same sensitive personal and company resources. To address this at the highest level, the tone at the top of organizations needs to be consistent and firm regarding acceptable mobile device use. A solution for business enterprises must include cross-functional governance channels to redesign the way enterprise mobility is treated from a security perspective, while at the same time ensuring the solutions meet individual user demands to encourage adoption and compliance. Tactically, organizations should follow the component solutions below to address the challenges introduced by the mobile risks detailed above:

1. Understand the current and future mobile use case to be enabled at an enterprise and consumer level
2. Identify sensitive resources and information assets that are becoming available through mobility solutions and channels
3. Determine if these elements have been vetted and approved by the proper cross-functional channels
4. Create policies and procedures to design leading practices as it relates to enterprise mobility
5. Enforce the mobility function on an ongoing basis through a fully enabled MDM tool
6. Monitor controls using device security and management platforms (i.e., MDM) and monitor for compliance
7. Incorporate proper governance into the mobile program to continuously identify, manage, and mitigate risk

For more information on how your company can benefit from KPMG's Emerging Technology Risk Mobility Services, please contact:

Francis Beaudoin
National Leader,
Technology Risk Consulting
T: 514-840-2247
E: fbeaudoin@kpmg.ca

kpmg.ca

The information contained herein is of a general nature and is not intended to address the circumstance of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.