
At the end of 2017, over 9 million customers found themselves at major risk after a hacking attack on a large mobile company. Security failures like these cost companies millions of dollars and thousands of customers every year.

With the steady growth of mobile use, smartphones and tablets are becoming the primary targets for attackers and malware. Unfortunately, many enterprises are not doing enough to protect valuable commercial and personal data stored on their employees' devices from cyber threats. What are the major threats that take advantage of lax security? Let's find out.

## Top 10 Mobile Threats

- Inconsistent security for IPs on your network
- Malware and insecure third-party apps
- Lack of control over lost and stolen devices
- Employees not following corporate mobile security policies
- No separation of personal apps and corporate software
- Weak authentication
- Software not optimised for a wide range of employees' mobile devices
- Poor protection of data during non-working hours
- Difficulty in maintaining and monitoring all mobile devices used by an organisation
- Poor security due to devices running on different versions of various mobile operating systems

Do any of the points above ring true for your company? If so, it means that you may have gaps in your mobile security. The good news is Magora's experts have prepared a security checklist that will help you protect valuable data from web criminals.



+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk

magora

# Enterprise Mobile Security Checklist

Here are our tips on how to guard your business against online threats and data leaks:

- Allow only authorised users to access your network
- Implement a corporate mobile security policy
- Use special tools to ensure that all devices that access the network are properly secured
- Specify an IT mobile security policy and enforce it using tools to ensure devices that access data are secure
- Design an Enterprise Mobility System that incorporates the following functionality:
    - Ensures devices that access corporate data are secure
    - Wipes every device when an employee leaves the company
    - Protects important data from sharing (for example, prohibits copying and pasting data into private emails)
    - Gives access only to devices that comply with the company's security standards (for instance, blocks access to smartphones with jailbreak)
    - Enables employees to register their personal devices
    - Manages corporate devices, allowing system administrators to install applications and updates on a large scale
- Use two-factor authentication
- Encrypt data on company computers
- Do not force updates - give the employees some time to prepare for changes

As you can see, a lack of mobile security presents many risks and challenges. It is extremely hard to track the many dangers coming from corporate and personal devices that have access to your business's information. An integrated enterprise mobile solution can help you solve this issue, monitoring threats, ensuring timely updates and tracking all devices within the corporate network. If you are concerned about keeping your data safe and guarding your employees against malware and online fraud, get in touch with our experts. Magora specialists will advise you on the best data security action plan for your company based on the specific requirements of your business.

magora

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk