Fliplet
apps made easy

Everything You Need To Know About Mobile Security

Part of
The Complete Guide to Adopting Mobile and Apps in Your Company

The Complete Guide to Adopting Mobile and Apps in Your Company

This ebook is part of a series of guides covering all the key topics related to enterprise mobility.
Find the complete guide as well as the individual sections at **fliplet.com/ebooks/**

Mobile Security

Everything You Need To Know About Mobile Security

Mobile App Benefits

The Benefits and Uses of Mobile Apps

App Development

5 Easy Steps To Building Your Own Mobile Apps

App Distribution

How To Share Your Apps With Employees & Customers

Mobile Business Case

Building A Business Case Around Your Mobile Strategy

Introduction

For IT the #1 weakest link in security is seen as mobile devices. This is an understandable concern if you consider that **5.2 million smartphones were lost or stolen in the US in 2014.**

In this section, part of our Complete Guide to Adopting Mobile and Apps in Your Company, we cover the main threats to security and how they can be combatted through mobile security technology. Understanding the risks will better equip you to either choose the appropriate technical solution or participate in internal discussions with the relevant team.

The section gives you an overview of some of the security concerns and solutions that should be kept in mind, but your IT team will be able to advise you on the exact needs depending on the nature of the apps you are creating and the data they will include.

Security risks

Securing how employees can use mobile devices and apps to access corporate content is becoming increasingly important, especially with the proliferation of **Bring-Your-Own-Device (BYOD)*** initiatives where employees can use their own devices, which may not have any security software installed.

The table below outlines the major risks that the use of mobile can create and how these can be mitigated.

Bring-Your-Own-Device (BYOD) - A policy which allows employees to use personally owned mobile devices (laptops, tablets and smartphones) for work and to access corporate information and applications.

Risk	Solution
! Sensitive data is leaked via unprotected apps or networks	› Encrypt all data passing between the network and the user's browser › Limit mobile devices to access only certain safe resources, such as corporate email or internal documents › Block undesirable apps from being downloaded
! Employees leave the company and still have access to corporate apps on their mobile devices	› Delete mobile data contained on the device remotely › Remotely lock down the app until the device can be fixed › Implement a login system that ensures the account belongs to a valid employee
! Mobile devices are lost or stolen	› Require users to regularly change the password on their mobile device › Delete mobile data contained on the device remotely
! Sensitive data contained in mobile apps is accessed by external partie	› Add additional layers of security and password protection to apps › Use enterprise app stores to distribute apps privately to employees only

How can devices be secured?

Your security device requirements will depend on how sensitive data is. There are three main options:

1. **The user is responsible for their own device**. This usually involves educating users on how to secure their device, but involves no complex IT systems. This is usually the option taken by organisations that are not heavily regulated, as the risk of lost data to the company is limited.

2. **Certain built-in security features are required**, such as device locks (passcodes, pattern codes, touch ID) and device encryption. This can be enforced through training, manual checks or setting policies with software, such as a mobile device management system (MDM).

3. **Additional security is provided by a Mobile Device Management (MDM) system.** An MDM system provides additional security features that can be controlled by your IT department, such as device encryption, password strength standards, auditing and many other security features. This solution is recommended if the data accessed by devices and apps is of a sensitive nature or the above solutions are not suitable for your company or organisation.

How can apps be secured?

There are many options available when it comes to securing app data. The main areas of focus are:

1. Distribution

App distribution involves ensuring that users can easily access and download apps without compromising the security of their data. Security requirements will vary depending on whether apps will be distributed via the public app stores or a private enterprise app store.

Public app stores

Companies often share apps with employees by submitting them to public app stores and asking them to use a login for access. But this may not be the most suitable option if the app contains sensitive data or if you want to have control over who can download the app. In that case, a private enterprise app store will provide better security.

Enterprise app stores

The main benefit of enterprise app stores is that they ensure apps can only be downloaded by people who are given access, often employees. Using an enterprise app store rather than the public app stores also means that apps are not subject to the public app stores' guidelines for submission and approval times, that can take as long as 15 days for Apple.

A few less obvious and often overlooked benefits of enterprise app stores are:

- They group all apps together in a single location so that employees can easily access them and discover what other apps are available

- They allow you to have control over who has access to which apps and to keep track of how many employees are using apps. Built-in tracking of downloads and usage help to ensure apps are being used by the right users in the right way

- They allow for apps to be automatically installed on users' corporate devices.

These benefits make for a much more convenient app distribution process that can be managed internally.

2. Logins and passwords

Logins provide additional app security by requiring users to enter a password when they want to access an app.

Logins are ideal for apps containing highly sensitive data, as this is yet another layer of security on top of device locks. Logins should also be used if the app is going to be distributed in the public app stores or if you want to have tight control over who can access the app.

If the data contained in the app is not of a highly sensitive nature, logins may not be appropriate as they could inhibit employees' user experience.

Password policy and Single Sign-On

To decrease the chances of hacking and virus attacks, a password policy can be implemented, requiring employees to set strong passwords for their mobile devices and to change them regularly.

Single Sign-On (SSO)* is a secure and convenient way of doing this because it allows employees to log into all their apps and accounts using a single password and it enables IT to centrally manage all accounts.

3. Network and data encryption

Network encryption

Network encryption secures all data passing from a mobile device to a server and back, preventing external parties from being able to read it. Common types of encryption include **Virtual Private Networks (VPN)*** or **Secure Socket Layer (SSL)*** depending on the type of service that needs to be secured.

It is also important to ensure that the servers storing app data are secure.

SSO (Single Sign-On) - An authentication technology that allows users to enter one username and password to access multiple apps or accounts. For example, using Google or Facebook details to sign into news or media websites.

VPN (Virtual Private Network) - A VPN allows the creation of a private network that users can access even if not connected to their corporate network. For example, when users are travelling or working remotely they can connect to their company's private network to access necessary files and data.

SSL certificates - A security technology used to encrypt network transactions and communications. For example, payment transactions on e-commerce websites are often encrypted using SSL.

Device encryption

Your company may also benefit from encrypting the app on the mobile device. This means that if the device is lost, the data on the device cannot be accessed with an app username and password. Instead, the account can be disabled centrally, rendering the thief unable to access the app.

Security audits

Full security audits, which assess the device's health and highlight if the mobile device or app is affected by a security issue, can be done remotely.

They can be conducted either by your internal IT team or external security professionals and can establish if data is at risk, check for any security gaps and determine if additional measures are required.

Partial or remote wipe

MDMs offer the ability to wipe all corporate data remotely from a mobile device. This means that if an employee loses their mobile device or if they leave the company, all sensitive app data can be deleted – and if the mobile device is found, content can easily be restored.

MDMs also allow for only corporate content to be deleted, leaving personal content untouched. This is highly desirable particularly in the case of companies running BYOD initiatives where employees use the same mobile device for work and personal tasks.

Key questions and considerations:

- How and where will mobile devices and apps be used?
  What data will be used on the mobile devices?
- What security is right for your business and users?
- Are there existing systems used by your company that can secure the apps, such as MDM or **Mobile Application Management (MAM)***?
- What questions and tests need to be reviewed before each app is launched?
- Is app data secured on mobile devices?
- Are transactions between mobile devices and servers encrypted?
- How can the impact security measures have on user experience be minimised?

MAM (Mobile Application Management) - A software used to secure, manage and distribute mobile apps in the enterprise.

Mobile is not the future, it is the now.
Meet your customers in the environment of their choice, not where it's convenient for you.

Cyndie Shaffstall, SpiderTrainers

About Fliplet

At Fliplet our mission is to revolutionise how companies use mobile by helping them to streamline business processes, increase productivity and improve communication between employees.

So we created an enterprise app builder that allows anyone within your company to create and distribute enterprise apps quickly, securely and with no need for development skills.

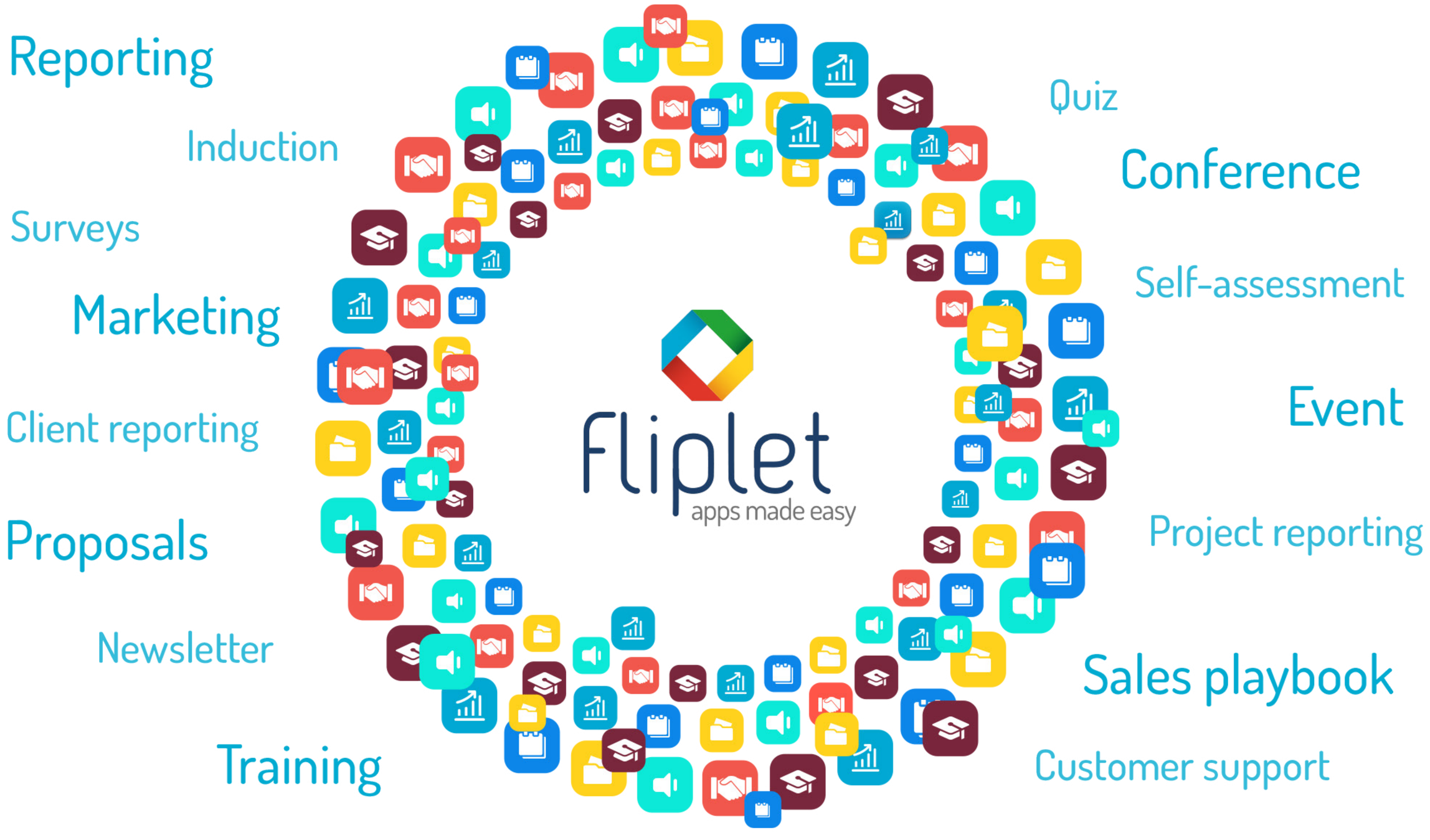
Using Fliplet, you can create enterprise apps in a variety of departments, including:

- Sales
- Marketing
- Events
- Internal communications
- Reporting
- Training
- Project management
- Health & safety

Enterprise apps are the future of business – don't let yours get left behind. Head over to our website fliplet.com and start your free trial now.

“We’re democratising the app revolution”

Ian Broom, Fliplet CEO & Founder



Learn More

UK Office **+44 020 3582 9720**
US Office **+1 (415) 200 3720**

http://fliplet.com
hello@fliplet.com