TIPS TO AVOID THE SEVEN DEADLY SINS OF MOBILE SECURITY

A secure and productive mobility strategy is a game changer for any business in today's connected world. It's becoming more imperative for users to gain access to corporate data on their mobile devices both inside and outside of the corporate network.

Mobile workflows can be faster and more intuitive than those on desktop computers, but enterprises need to be cautious before allowing the widespread use of sensitive business information on unsecured mobile devices. In many cases, unfortunately, that means user productivity is overlooked in IT's pursuit for data security.

Fortunately, businesses are no longer required to sacrifice usability for security. Below are the "seven deadly sins of mobile security," along with tips on how to best avoid or tackle them so usability and security aren't pitted against each other.

01 AVOID RELYING ON DEVICE MANAGEMENT ALONE

Let's be clear, Mobile Device Management (MDM) is not a comprehensive security solution; it's a device management solution. While MDM is a good option for securing corporate devices housing corporate data, bring your own (BYO) and corporate owned, personally enabled (COPE) scenarios are cases where a containerization approach is a much better fit. A containerization approach to mobile security is a major benefit to businesses looking to protect corporate data on devices that hold a mixture of corporate and personal data on them.

Look for a secure container solution that provides app-level, device-independent encryption which secures corporate data while keeping personal data separate. This provides advanced protection regardless of device ownership and management status.

02 DON'T SACRIFICE USER EXPERIENCE ON THE ALTAR OF SECURITY

As more content and applications are being mobilized and mobile devices replace laptops and desktops as our primary computing sources, there needs to be a much greater emphasis on user experience. Apps need to be easy and compelling to use for the experience to be successful. Security controls that hamper positive user experiences, especially on personal devices, will encourage users to find other, often less secure, ways to access corporate data.

Security needs to be a foundation underneath your application, not a cage around it. Look for development platforms that allow you to build applications on top of a solid security footing that hides the details from the user and abstracts the complexity for the developer and administrator. Doing so allows you to deliver applications that are both highly usable and highly secure.

03 AVOID PROTECTING CORPORATE DATA WITH PERSONAL PASSCODES

Passcodes are not a "one size fits all" item. Using just one device-level passcode means that the same level of authentication stands between a user and his game of Angry Birds as between him and your sensitive corporate data. Using a simple passcode means that your data is at risk but using a more complex code will get in the way of the user performing common, every-day tasks and will hamper user acceptance of your mobility strategy.

Look for solutions where apps and their data are protected with passwords and cryptography that is independent of any underlying device-encryption. This will give you peace of mind as the app data will still be encrypted even if a device passcode is hacked.

04 STOP OBSTRUCTING BUSINESS WORKFLOWS

Users want to do their jobs as quickly and effectively as possible. And in today's mobile-cloud world, if they don't have the tools they need to do it then they will find another way. Inevitably this will lead to "shadow IT," where users find their own solutions using consumer-grade tools over which you have no control.

As you roll out your mobility strategy, it's important to ensure that users have easy access to the full set of apps they need. For example, having mobile email, but no ability to edit, print, save and share Office attachments will result in incomplete workflows. Look for a solution that not only allows you to manage the data, but also ensures that the apps work seamlessly to provide the whole workflow that the user needs. The user doesn't just need the apps; those apps have to work together, securely sharing both data and services among them to make the user's job easier, not harder.

05 DON'T TREAT SECURITY INCONSISTENTLY ACROSS PLATFORMS

One thing that is certain about mobility is the diversity of devices and operating system versions. And while different roles or use cases such as a kiosk tablet vs. a sales person's personal smart phone might necessitate different security policies, the device capabilities itself shouldn't drive your security policy. Operating system diversity and fragmentation, especially for Android, is one of the main challenges for IT. And in the mobile space, diversity and the lack of a common security paradigm can cause a lot of problems.

A device-agnostic secure mobility solution can help cure these headaches. A secure container can raise the security of all devices up to the same, high level, especially important for BYO and COPE device ownership models. Mobile device management (MDM) relies on the native device and OS security capabilities. Design your mobile security strategy around use cases and roles, proactively setting your security policies as appropriate instead of letting the device and OS capabilities choose it for you. This allows you to have confidence and control over corporate data while allowing device choice for users.

06 DISALLOW DATA TO LEAVE YOUR CONTROL

Data needs to move around to be useful, whether it's moving between applications, between devices or between users. However, data breaches often happen when data is moved outside of the control of IT-approved policy configurations. You need to make sure that you keep control of the data as it moves and that it does not end up in some unsecured app.

The right mobile app security solution must allow a business to determine how data moves into, out of and around the enterprise domain. Containerizing this data and applying shared workflows helps keep data within the confines of the business. As the data is segregated, it also makes it possible to remote wipe any corporate data in the case of a crisis, a lost or stolen device or employee termination.

07 SECURITY DOESN'T STOP AT THE EDGE OF YOUR ENTERPRISE

Your need to secure data doesn't stop at the edge of your enterprise. Whether you are sharing data with your suppliers, business partners or franchisees or if you are giving your customers, patients or citizens access to business systems, your data is going to need to make it onto devices outside your organization and with that data comes a need to secure it.

Look for a mobile security solution is flexible enough to secure the use of sensitive business information wherever it goes. It needs to be able to cope with identity models that go beyond your corporate Active Directory, and it must continue to offer security even when the devices are ones that you will never be able to manage yourself – your suppliers, business partners, customers and even employee's BYO devices.

As mobile devices get more powerful, they enable us to be ever more productive. Our corporate mobility solutions need to grow as the platforms grow more capable, and they need to evolve to fit usability and security requirements for both IT and users. Enterprises looking to secure mobile apps and corporate data should look out for the seven deadly sins of mobile security to ensure a strong user experience paired with an efficient data protection strategy.

ABOUT GOOD

Good Technology is the leader in secure mobility, delivering solutions across all stages of the mobility lifecycle for enterprises and governments worldwide. Good offers a comprehensive, end-to-end solutions portfolio, consisting of a suite of collaboration applications, a secure mobility platform, mobile device management, unified monitoring, management and analytics, and a third-party application and partner ecosystem. More than 6,200 organizations in 189 countries use Good Technology, and we are trusted and deployed in 100% of the FORTUNE® 100 commercial banks and aerospace and defense firms as well as leaders across healthcare, manufacturing and retail. Learn more at **www.good.com**.

Global Headquarters
+1 408 212 7500 (main)
+1 866 7 BE GOOD (sales)

EMEA Headquarters
+44 (0) 20 7845 5300

Asia / Pacific Headquarters
+1 300 BE GOOD

©2015 Good Technology Corporation and its related entities. All use is subject to license terms posted at www.good.com/legal. All rights reserved. GOOD, GOOD TECHNOLOGY, the GOOD logo, GOOD FOR ENTERPRISE, GOOD FOR GOVERNMENT, GOOD FOR YOU, GOOD DYNAMICS, SECURED BY GOOD, GOOD MOBILE MANAGER, GOOD CONNECT, GOOD SHARE, GOOD VAULT and GOOD DYNAMICS APPKINETICS are trademarks or registered trademarks of Good Technology Corporation and its related entities. All third-party trademarks, trade names, or service marks may be claimed as the property of their respective owners. Technology and products belonging to Good are protected by issued and pending U.S. and foreign patents. Content: 07/15 I Rev. 31JUL2015