Developing a mature enterprise mobility strategy

Once every 20 - 25 years the information and communication technology (ICT) industry shifts to a new technolo platform for growth and innovation. The Industrial Development Corporation (IDC) calls it the third platform, built on mobile devices and apps, cloud services, mobile broadband networks, big data analytics, and social technologies. These paradigm shifts are affecting organisations worldwide.

By Neil Cosser 11 Jul 2015

Neil Cosser

From 2013 through 2020, IDC believes that 90% of IT industry growth will be driven by third platform technologies that currently represent 22% of ICT spending. While each of the third platform technologies impacts organisations around the world in countless ways, mobility is one of the most disruptive trends that the enterprise has had to deal with in a long time

Mobile access to everything

Enterprise mobility or bring your own device (BYOD) as others call it, is prevalent and is set to grow. The latest report fron IDC research states that 40.7% of devices used by information workers to access business applications are personal resources including home PCs, smartphones and tablets such as Apple's iPad.

In the past, enterprise mobility meant employers are providing their employees with mobile devices to improve personal productivity. Fast forward to 2015, enterprise mobility involves empowering users with the tools they need to be productive Users are demanding mobile access to everything and because of that enterprise mobility has moved from just beyond embracing various devices to creating an open and combined system of cloud, analytics, secure networks and devices.

Introducing new security risks

The ease of access to company information is allowing companies to creating a platform for the deployment of mobile app With seamless access to information from different sources, mobile apps will allow business users to see a holistic picture activities. However, the rise of mobility and the increase of data and information stored on mobile devices also make users prime target for criminals. Much like the early days of the Internet or PCs, new mobile technologies are introducing new security risks. Hackers are now also targeting mobile phone devices and mobile malware.

It's important to block high-risk vulnerabilities by ensuring comprehensive security controls and policies are in place and a being effectively implemented. Multiple layers equal multiple barriers between data and potential threats.

Enterprises often allow for information to be accessed remotely via simplistic, insecure usernames and passwords. These can easily be compromised and access to corporate apps should, therefore, be secured by strong authentication measur to ensure access only to users with appropriate admin rights, using secure identity and access solutions such as One Tim Password (OTP).

It's also important to strike just the right balance between security and convenience. If security measures are too complex for instance, if it takes a user 10 minutes to log in - users will either find an alternative to bypass the security measures in place or simply not use the app. To ensure widespread and effective adoption, the balance between security and convenience is key.

The more factors of authentication the safer

Top-tier executives tend to be highly mobile but simultaneously have access to highly confidential data. When setting up security measures for these individuals, it would be prudent to introduce an extra layer of security by protecting their e-ma and data with the toughest encryption and access credentials. In this case, even if the device is lost or stolen, it remains secure and cannot be accessed if all authentication factors are not present.

The more factors of authentication that are introduced, the more secure the device. So another way to reduce threat surfa in mobile devices is to introduce a digital signature into the mix for specific data and business platforms. Organisations ca also implement the single-sign-on (SSO) to ensure secure access to web-based applications from multiple end points; the advantage here is that one login access to all systems without the user being prompted to log into each one again.

ABOUT THE AUTHOR

Neil Cosser, identity and data protection manager for Africa at Gemalto