Combatting mobile security breaches

Samsung Electronics South Africa notes that in today's high stakes corporate world, a data breach can cost an enterprise dearly. The damage caused could be financial, it may be reputational, or the news of such a breach may simply scare away potential customers. Whatever the result, a lack of effective mobile security can disrupt an enterprise, but the information should still be accessible to the legitimate user.

Image by 123RF

Smart-devices are particularly attractive to cybercriminals, due to the sheer number in use and the multiple vectors of attack they present, including malicious applications and Web browsing. Companies therefore need to understand the role mobility plays in their organisation and consider the risks it poses to their business.

“Samsung is aware of the many security issues raised by mobile devices and this understanding has been integral to the development of Samsung Knox, a security solution that offers multi-platform interoperability and a built-in, defence-grade security platform. It has been designed to keep business information intact, giving enterprises the opportunity to achieve organisational success in a more connected world,” says Paulo Ferreira, director of Enterprise Mobility at Samsung Electronics South Africa.

According to Ferreira, the mobile security challenge is now at the forefront of business leaders’ thinking. While threats targeting mobile devices have not changed, the severity of the consequences has increased dramatically.

“There are still two main causes of data loss on mobile devices: physical device loss and misuse of apps. Since mobile devices are now storing and accessing more-sensitive data, this means that in a scenario where a device falls into the wrong hands and does not have adequate protection, it can be the source of a major data breach,” Ferreira explains.

On the other hand, the challenge around the misuse of applications is mainly due to the fact that it is invasive. Often, the application requests permission to access the user's contact list, personal information and location. Furthermore, many employees use personal file sharing tools with corporate documents. In addition, since applications rely on the cloud, mobile devices running compromised applications will provide a way for hackers to remotely attack public and private clouds and access corporate networks.

Other mobile threats include the rapid growth in *malware* attacks and user error. The former poses a security challenge in that when a device that has been infected by malware connects to a network, not only is the malware able to propagate, but it is also often designed to steal data from devices.

In addition, user error is a further challenge. Many users are lax when it comes to securing their devices, using weak passcodes or none at all and not encrypting the data that they contain. Given that mobile devices are routinely lost or stolen, unsecured devices provide offenders with easy access to sensitive data.

Knox is supported by over 120 enterprise mobility management (EMM) providers worldwide and performs with all popular single sign-on (SSO) and virtual private network (VPN) solutions to preserve enterprise legacy IT investments.