EMBRACING BYOD

ARE YOU EXPOSING CRITICAL DATA?
Supporting User-Liable Devices

While several factors can be cited for the consistent strong growth of consumer smartphone and other mobile device usage in recent years, reduced cost of device ownership is primary. This, along with other factors, led to a significant increase in the smartphone penetration rate, as a recent Google-sponsored Ipsos study reported growth in all five countries surveyed.¹

The increased use of personally owned smartphones at and for work has also been causing problems for IT administrators, as unlike company-issued devices, these do not come with equipment device management features enabled. Consumerization is now being pursued in an attempt to increase productivity and reduce costs. As a result, compliance with previously existing IT policies may not always be a top priority.

Despite these IT-driven concerns and the potential security risks of allowing the use of personally owned devices, the bring-your-own-device (BYOD) trend has been gaining traction among several enterprises. IT administrators already grant access to internal resources such as corporate email accounts, contact lists, and intranets via personally owned devices.²

Mobile Device Usage in the Cloud Computing Era

Mobile devices are ideal for accessing cloud service platforms, which are increasingly being used by several organizations for their daily operations. Similar to other means of storing information, however, these can pose a different set of risks. The following are some of the cloud service types smartphone owners and/or organizations use at present:

- Note-taking apps
- Document-sharing or -storage services, which are normally used to share and manage documents
- Some cloud storage services, which allow businesses to completely host documents in the cloud

![Figure 1. Most common corporate applications accessible from personal devices](Source: Trend Micro Enterprise IT Consumerization Survey, June 2011)

---

What kinds of smartphone data can be lost?

Broadly speaking, the kinds of smartphone data that can be lost varies depending on how “smart” a device is. At the most fundamental level, information such as contact lists, text messages, and call logs can be found in any kind of cellular device used for company purposes. In isolation, this information may have relatively limited value to most businesses. Note, however, that it can be used to launch social engineering attacks.

At present, smartphones are invariably used to connect to corporate networks in order to gain access to email inboxes, calendars, and internal portals, which all pose severe risks to enterprises should their contents be leaked to third parties. Leaked email and attachments, in particular, have caused numerous organizations, at the very least, embarrassment in the past.

Attackers can use compromised or stolen mobile devices to access all kinds of information stored in them or in the networks or databases they have access to. Compromising an organization’s login credentials to any of the aforementioned services can also put its document databases at risk of unwanted exposure.

How can data stored on mobile devices be lost?

Two typical scenarios can lead to the exposure of data stored in mobile devices, among others—device loss or theft and not securely communicating via mobile devices. Certain malware such as DroidDreamLight, in fact, have been known to steal data from smartphones.3

Device Loss or Theft

Smartphone loss is, unfortunately, an already-too-common occurrence. Even though password and comparable lock features are part of all modern smartphone platforms, these still cannot be considered effective means of securing devices, especially those that contain sensitive information. Losing a smartphone comes with the expectation that malicious users can obtain access to all of the information stored in it.

Unsecure Mobile Access

Many mobile device users access the Internet via any available Wi-Fi network wherever they are. Accessing the web via open Wi-Fi networks, though free, may not be the best idea especially if confidential and sensitive information is stored in a mobile device. When mobile users access unsecure sites or make use of apps that are not properly configured for security, the possibility of losing data to malicious actors looms larger.

Data Loss Incidents Involving Mobile Devices

- A smartphone with access to a healthcare service provider’s official email and records was lost, affecting 900 people.
- An event organizer’s tablets containing customer information and payment records, including credit card credentials, were stolen.

Sources:

http://www.ukhealthcare.uky.edu/Default.aspx?id=9259
http://blog.eventbrite.com/our-commitment-to-security

3 http://blog.trendmicro.com/massive-code-change-for-new-droiddreamlight-variant/
What mobile device security solutions are available?

Though typical mobile device management (MDM) solutions offer remote wipe or lock options, enterprises should seek solutions that also aid in threat prevention and data protection. MDM solutions such as Enterprise Mobile Security[^4] would have the ability to minimize incidents of data loss or leakage.

Installing data protection solutions in critical systems, along with MDM solution use, is also a great measure to minimize risks associated with data loss or leakage. Should users lose improperly secured mobile devices that have access to or contain sensitive information, data protection solutions installed on internal networks and systems that provide authentication, audit, and access control capabilities can continue to safeguard an organization’s main data storage.

Enterprises looking to navigate the oncoming challenges of consumerization should develop a strategy that recognizes that employees will bring in devices into the corporate network. For guidance about how to develop such a strategy, read our Consumerization Blog[^5].

---


TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years’ experience, we deliver top-ranked client, server and cloud-based security that fits our customers’ and partners’ needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TRENDLABS™

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to continuously monitor the threat landscape across the globe; deliver real-time data to detect, to preempt, and to eliminate threats; research on and analyze technologies to combat new threats; respond in real time to targeted threats; and help customers worldwide minimize damage, reduce costs, and ensure business continuity.