

Mobile Security 2007: End Users Are Losing It

SKU: IN0703622MBM
Analyst: Bill Hughes
Bill.hughes@reedbusiness.com
+1.425.453.9917
March 30, 2007

Executive Summary

The security of wireless voice services and mobile data are key considerations for users and their employers. Based upon the results of our survey of 789 end users, a majority of users overestimates the risk, misunderstands the security threats that do exist, and looks for protection from sources that cannot help.

The current reality is that cellular voice and data services based upon digital technology are as secure as wireline networks, from a pragmatic view. From an organizational perspective, the efforts that protect information from wireline threats are the same as those that will protect information from wireless threats, with one exception.

That exception is the possibility that user equipment in the field can get lost or stolen. Users tend to overestimate their ability to maintain control of mobile equipment, and with it, its access to sensitive corporate data. This survey finds that the average individual will lose a mobile handset only once in more than 25 years, but that extrapolates to over 8 million devices in 2007. Furthermore, smartphone users, the ones with the most access to sensitive information, are 40% more likely to lose a device.

Since it is impractical to “put the genie back in the bottle” and limit access to corporate information to landline connections, organizations will need to find a way to educate users about the facts of wireless security. This is an opportunity for the direct sales forces of carriers to use security education as a tool to differentiate their offerings through this value-added service.

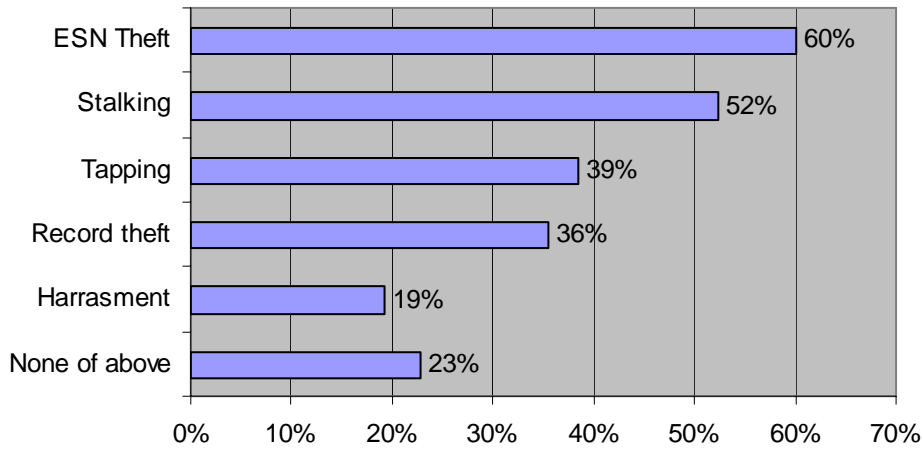
Frequently training on security is dry and boring. However, the degree of misunderstandings about mobile security threats could make addressing this subject very enlightening. For example, Figure 1 presents the concerns expressed by wireless voice users. A majority are concerned about ESN theft through the “cloning” of their phone’s information and the ability of stalkers to track their location.

The problem is that carriers have already addressed these situations for the better part of a decade. Users are just not aware of this.

HIGHLIGHTS

- Most mobile users have security concerns about their mobile phones. Many of these concerns are about problems that have already been solved.
- The bigger problem for security breaches involves the loss of mobile phones, particularly smartphones. Smartphone users lose their devices 40% more often than mobile phone users
- Too many organizations allow users to decide what technology they will use for mobile data, regardless of security implications. This is a risky approach. Mobile devices should be centrally managed by businesses.
- Carriers should differentiate their offerings through security training for their customers.

Figure 1. Voice Security Concerns among Wireless Voice Users



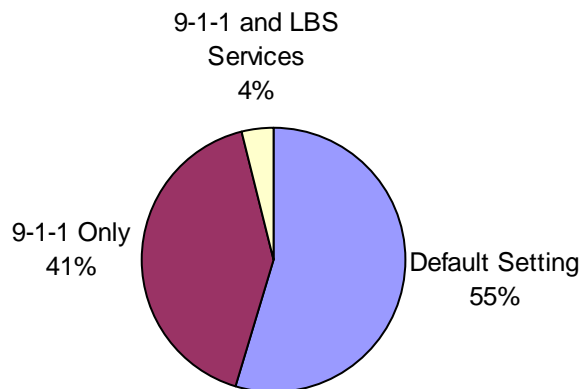
Source: In-Stat, 4/07

n=773

Compounding the security problem is that users reject even minimal steps to increase security. For example, only two-thirds of users are willing to accept that the carrier can disable their mobile device if lost or stolen. One-third finds this basic carrier service to be unacceptable. The increased use of passwords is unpopular, as are restrictions to calling area.

In addition, many security experts find that users keep the default password on their voice message service and on their mobile devices, an obvious security lapse. Supporting this opinion are the results presented in Figure 2. Modern CDMA phones offer a setting on whether to send location information on the phone, which can be set to send information to E9-1-1 only or for E9-1-1 and location-based services (LBS). The results in Figure 2 show that most users were not aware that there was this option.

Figure 2. Settings for Sending Location Data among CDMA Phone Users Concerned with Stalking



Source: In-Stat, 4/07

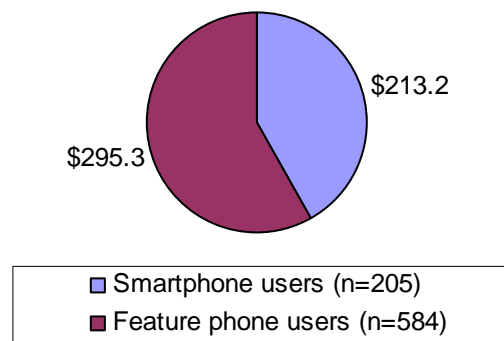
n=312

When it comes to mobile data security, users are more alert to threats, and for good reason. While wireless voice involves end-to-end communication, the value of mobile data comes from its ability to

connect to a variety of sources and access large databases very quickly outside the physical confines of an office. While the actual number of security breaches from mobile phones have been blessedly few, to date, it is unlikely that this will be the case indefinitely.

If we just look at the projected value of lost mobile devices, we see that smartphones represent a disproportionate value of lost hardware. This does not include the value of data that could be accessed should an organization not know about the loss because the user does not tell his employer that his device is lost and has access to sensitive databases.

Figure 3. Projected Value of Lost Mobile Devices in 2007



Source: In-Stat, 4/07

A solution to this problem is for carriers to encourage the use of mobile device management systems. These have the tools to disable or “wipe” a mobile device if it is lost. These systems can also give the organizations greater security in protecting call records. These services protect corporate information in a way that piece-meal security systems do not.

The first step for organizations to get in front of mobile security is to assume corporate liability for mobile communications. As long as users are left to make network decisions, the solutions will be the most expedient or least expensive, not necessarily the most secure. If wireless carriers fail to make this case and acquiesce in letting corporate customers pursue individual liability as an acceptable option for business use, it seems inevitable that security breaches will become more common.