Renegade Smartphones Threaten Business Security

by Sharon D. Nelson, Esq. and John W. Simek

OK, the smartphones really aren't the renegades – their users are. Unfortunately, the users have gone off the reservation in a major way, faster than anyone imagined, and with grave security implications for law firms and all businesses.

Consistently, the trade press is reporting that concerns about smartphones are outrunning concerns about cloud computing, which has for several years been a major worry for security specialists.

Are there ways to control the use of smartphones and tighten security? Sure – and they are usually employed by large-scale enterprises. Are small businesses using them? Almost invariably the answer is no.

Most analysts agree that, among smartphones, the BlackBerry and the Windows Mobile phones provide the best inherent level of security. The BlackBerry is considered especially powerful because it provides confirmation of remote wiping, which could be critical in the event of a data breach.

For other devices, or for companies that are supporting multiple smartphones, there is management software from vendors such as Credant Technologies, Good Technology, Sybase, Trust Digital, Trend Micro and MobileIron, among others. These platforms offer centralized control of:

- Password management (complexity and history).
- Authentication authorization.
- Strong encryption of the device and any inserted memory cards if available.
- Inactivity timeout, in which users are logged out of an application session after a specified period of inactivity (often 5-10 minutes) and are prompted for a password to resume.
- On demand remote wiping.

- Authorized applications that can be installed to the phone.
- Features access (e.g. disable usage of the camera for pictures and/or video)
- Automatic wiping if a device is lost or stolen or if the user (or someone in possession of the user's phone) enters the authentication credentials incorrectly a specified number of times.

As some wags have noted, even plastered out of your gourd, you ought to be able to get the password right in 10 tries.

In contrast to the BlackBerry, the iPhone is considered vulnerable because, if the SIM card is removed, the phone cannot receive a remote wipe command and it is child's play to bypass the configured PIN. We thought Apple had resolved the PIN bypass problem with the iPhone 4, but German researchers have demonstrated the continued insecurity of the iPhone. They are able to extract stored passwords from a PIN protected, encrypted iOS 4.2.1 device is six minutes with publically available tools.

Even with the PIN bypass issues, the iPhone is considered less insecure with respect to malware than the Android smartphones. According to a recent report by Trend Micro, Google's Android operating system for mobile devices is the the most vulnerable to hackers and malware. Steve Chang, chairman of Trend Micro, said "Android is open-source, which means the hacker can also understand the underlying architecture and source code." Obviously, this understanding gives the hacker a serious advantage when contemplating mischief.

It is critical, no matter what platform is used, that users cannot disable or significantly modify any of the security features, because you can bet the mortgage that they'll try.

Having said all this, none of the possibilities for hardening smartphone security will work if no one takes the time to implement them. We are hard-pressed to think of smaller firms we have seen that have adopted these measures.

Employees have been anarchists for quite a while, visiting (unless technologically impossible) sites forbidden by policy, streaming music and videos, again often in

violation of policy and choosing not to employ passwords to access their phone whenever the firm's security permits that option.

Not all problems can be laid entirely at the feet of employees. The rise of malware for smartphones has been a recent alarming phenomenon. Only two years ago, there were only 400 documented pieces of malware for phones (versus millions for computers). It appears that that two years ago was really "the good old days" of smartphone security.

Pretty much any device with a browser and access to the Internet is at risk. Merely clicking on a link or visiting a website may infect the phone by installing malware that has the potential of gathering data and transmitting it to another location without the user's knowledge. Some would say "So what? I don't store any confidential client or personal data on my phone." What about e-mail access? Primarily, smartphones are used for application usage and e-mail access. If you have an infected phone, just opening an e-mail message could be sending its contents to another person.

Because of some of the security deficiencies noted above, security firm McAfee has predicted that iPhones, iPads and Androids will be major targets for cybercriminals in 2011. McAfee predicts that the cybervillains of the world will begin setting up botnets for Apple devices to distribute malware and launch cyberattacks. They are also expected to begin developing Trojans specific to those devices. Geolocation features in social media websites, which are also available on smartphones, will further compound exposure to cybercriminals according to McAfee.

To the extent that users do not use smartphones securely, they will make themselves targets of the bad guys and potentially expose their employers' data, however innocently. A lot of this is occurring because of the "consumerization of technology," where what consumers want/buy/are absolutely determined to use begins to drive businesses to adopt those technologies.

Mind you, those technologies are darn useful, as some very major players have discovered. But there remains considerable tension between those who are

devoted to their incredibly slick devices and those who are responsible for information security. It is not a question of whether cybercriminals will steal data from businesses with unsecured mobile devices – it's just a question of how much and when it will happen.

Another component to the problem is the smartphone manufacturer. Already, Apple has been sued for allegedly allowing iPhone and iPad personal data to be sold to advertising networks. Geolocation data could also be sold.

Some experts have pointed out that Google may be an even bigger problem than Apple given the amount of personal data, including geolocation data, that it collects.

Social media is also a player here, as many people reveal what devices and applications they use through social media, making themselves likely victims of targeted attacks.

What businesses need to do to remain safe is to standardize the apps that may be downloaded to company phones and to use technology to prohibit non-company phones from connecting to the network. Popular? No. And we're not likely to see this adopted at the small firm level anytime soon.

But the truth is that once you're behind the firm's firewall, it is both the right and duty of those in charge of security to impose reasonable controls. Where this gets especially dicey is where the employees own the phones, but the firm attempts to exert control. It is exceedingly likely that these attempts will result in an angry backlash from those who feel it is their right to do what they like with their smartphones.

The policymakers tend to fall behind with smartphones too. Many firms have policies forbidding the transfer of sensitive data to smartphones, but neglect to address taking photos at work or recording a firm meeting. Does the policy cover personal phones? How many times have you seen someone with a company phone in their left pocket and a personal phone in their right pocket? Even if there are policies, will the employee conform to them?

Things are happening very fast out there. Witness one recent study of 300 companies in the U.S. and Europe by Good Technology Inc., a vendor of mobile security and management tools. Nearly 80% of the respondents reported an increase in the number of employees who wanted to bring their own devices into the workplace in the past six to 12 months, and 28% reported a data breach because of the use of an unauthorized device.

And yet companies have been slow to recognize the security threats presented by smartphones, even though their lawyers are dutifully explaining to them that they are liable in the event that those smartphones cause a data breach. This awareness is dawning rapidly and we are sure to see a lot of scrambling as companies attempt to come to grips with this new threat to data security.

Most striking of all is a dawning perception among IT professionals and security experts that we have a new and compelling definition of smartphones: They are now computers that happen to be able to make phone calls.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com