

Being Smart About Smart Phones

Upper management has smart phones? They were bought with no input from the security manager? Well, how bad could it be? Oh, right, very bad. By C.J. Kelly

I LIKE TO think that not very many things can surprise me. But recently I got a big surprise that seemed to come out of nowhere, and it wasn't that I had won the lottery.

The IT department let me know that the help desk had been asked to install client software that would allow e-mail to synchronize with upper management's new smart phones.

Upper management has smart phones? Why didn't anyone tell me that earlier?

My fault, really. We don't have a specific security policy for mobile devices. Of course, we hadn't needed such a policy because this state agency has never been all that mobile. It just goes to show that you can never be too prepared.

Had a policy been in place, we could have avoided what has turned into a security problem that's hard to fix because upper management has a vested interest. We could have avoided the problem by setting requirements for devices like smart phones that would have satisfied my security concerns. With no policy in place, managers got what was cheap, with no real clue about what the security implications might be.

And what are those implications? For starters, these smart phones require client-side software that hooks into Microsoft Outlook, and for synchronization to occur, it seems that the user's PC has to be left running with Outlook open.

The list grows from there. E-mail transfers aren't encrypted. The phones aren't password-protected. They can't be managed remotely so that data could be wiped clean if one were lost or stolen.

But the worst thing of all, from my perspective, is that e-mails are cached on the Internet service provider's servers for up to seven days. That particular feature lets smart-phone owners access their e-mail via the Web.

That's a big security hole with dubious benefits. I mean, if you can get your e-mail at work or home and you are traveling with a smart phone, why do you need another alternative? We talked to the ISP's representatives and told them we did not want e-mail cached on their servers. Their answer: "That's the way it works." I was striking out.

I told my boss about my concerns, but he said management wanted smart phones. You can't really argue that point, but I wanted to document the risks we were opening ourselves up to, so that management would know just what was at stake.

Meanwhile, I started to explore the idea of upgrading to phones that would meet my security requirements. Yeah, it could be done — at twice the price. Is this some vendor plot?

**SECURITY
MANAGER'S
JOURNAL** 

What We've Got

Our managers are actually using two different models of the Palm Treo, the 650 and the 700p. Of those, the 650 is worse, but neither offers everything I want.

The Treo 650 seems like a good phone for a consumer or a small-business user. You can use it to surf the Web, send photos, read and send e-mail and text messages, and, of course, talk. You can also use it to access your computer remotely, and that gives me the security willies.

Clearly, some smart phones are smarter than others. So are some security managers, I guess.

Then there's that client-side software. I wouldn't object if it were used solely for syncing the device when connected to the computer. But having to keep a computer running to make sure the phone does what it's supposed to do is a real problem.

The Treo 700p offers more of what we need. Palm says that this smart phone uses a Secure Sockets Layer protocol to synchronize with an Exchange server, which eliminates the need to leave the user's PC running and provides the necessary encryption.

However, our state e-mail SSL certificate is apparently not compatible with or can't be added to the phone's list of acceptable certificates. So the phones can't connect directly with the state e-mail system. That seems like a problem that could be corrected by the phone vendor, but we aren't hearing the vendor say it will solve that problem for us.

What's more, we've had nothing but hardware problems with these phones, including spontaneous rebooting and intermittent synchronization.

So, what are the alternatives? Well, Palm's Web site tells me that the Treo 700w and 700wx "deliver everything you need without compromise." Ah, great, because I feel as if we've compromised our security rather severely with the phones we have. Our IT department tells me that we can get remote management software for these phones. That's certainly a plus.

Clearly, some smart phones are smarter than others. So are some security managers, I guess, since I'm now scrambling to care of all of this before we have a real security disaster on our hands. It all could have been handled ahead of time with a formal requirements-gathering and then a quick assessment of the best tool that would meet both IT and security needs. That didn't happen, and now I'm kicking myself.

This is where we stand: I have contacted the ISP's reps and have let them know that the Treo phones we have don't meet our technology or security standards. I have asked for a trade-in for the better phones, and I'm hoping we can arrange for a substantial discount. I await their proposal.

Meanwhile, potentially sensitive agency e-mails are sitting on servers somewhere "in the cloud." You know, this would be a really good time to win the lottery. ▸

WHAT DO YOU THINK?

This week's journal is written by a real security manager, "C.J. Kelly," whose name and employer have been disguised for obvious reasons. Contact her at mscjelly@yahoo.com, or join the discussions in our security blogs: computerworld.com/blogs/security.

To find a complete archive of our Security Manager's Journals, go online to computerworld.com/secjournal.