Boston Business Journal

April 19, 2013

Companies get tough as gadget risks spike

Mary K. Pratt, Special to the Journal

Steve Snyder, the chief information officer for the Massachusetts Convention Center Authority, knows the workers in his organization cover a lot of ground on a typical day. So he equips them with iPhones and iPads, allowing them to work as they move around the MCCA's 1.7 million square feet of space.

But there are limits to what he'll allow.

There are work applications on the devices, but no data is actually stored on them. Users must enter passwords to activate their devices, and they must do so again if they've left their smartphones or tablets idle for more than five minutes. He also uses mobile-device management software, which allows him to erase any data on any device that is lost or stolen.

Snyder said he still worries more about hackers trying to break into the MCCA's primary, back-end network, but he acknowledged that mobile devices present new concerns when it comes to protecting the corporate environment.

"If you have a device where you don't enforce these rules, then someone could do real damage," he said.

The financial security risks posed by mobile computing have exploded with the advent of smartphones and tablets that are increasingly essential to the way modern businesses operate. Indeed, Gartner Inc. predicts that 1.2 billion smartphones and tablets will be bought worldwide this year.

So organizations that once had only desktops and a few laptops now must contend with workers at every level using a variety of devices to email clients, collaborate on projects and complete transactions with customers and suppliers. And for many workers, those operations are being conducted with same device used for family photos, personal web browsing and an occasional game of Angry Birds.

"The primary risk is really the fact that these devices are small. Everyone carries them around, and they get left behind, lost or stolen," said Paul Hill, a senior consultant with Sudbury-based SystemExperts Corp. And without proper security measures, a forgotten or stolen smartphone or tablet could contain all sorts of sensitive data that could be exploited, Hill said.

IDC Research Inc. in Framingham recently pinpointed 1,000 examples of malicious mobile-gadget codes introduced between 2004 to 2010. In 2011, the flow of malware surged to 6,000 examples. Last year it exploded to some 36,000 examples, according to Stephen Drake, program vice president for mobility and telecom at IDC Research Inc. in Framingham.

“A lot of these apps are perfectly functioning apps, but there’s malware running in the back,” Drake said. He said the costs associated with such attacks are significant, and for a single organization can easily total in the tens of millions of dollars.

And it’s not just losses from theft that have companies worried. In September, Massachusetts Eye and Ear Infirmary agreed to pay $1.5 million to settle allegations leveled by the U.S. Department of Health and Human Services after a doctor lost a laptop containing medical records for roughly 3,500 patients. Four months later, the former owners of medical-billing concern Goldthwait Associates in Marblehead and four other local medical practitioners agreed to pay $140,000 to settle allegations brought by the state’s attorney general that they improperly managed patient data, some of which was stored and accessible through mobile devices.

Enterprise IT departments are striking back. The most common weapon is mobile device management software, which gives companies the ability to, among other things, remotely wipe data from lost or stolen devices.

Companies also are adopting technologies that create virtual barriers, such as so-called app wrappers, that partition mobile devices to allow for work applications to be separate from the user’s personal activities and data.

Drake said IDC studies show that 40 percent to 50 percent of IDC’s own corporate customers have some sort of mobile-device management, up from the single digits just several years ago. But that still leaves about half of all enterprises with little or no protection.

“There are products out there to help with this, but there’s no silver bullet,” said Tyler Shields, a senior researcher at Burlington-based Veracode Inc., which provides application-security testing.

He said companies that aggressively track mobile security are “extremely few and far between.” And even the best are still susceptible to the mobile arena’s weakest link: human error.