

Mobility and security need to mix

This must be the mobile decade. Everybody and everything is on the go, in the cloud, over the air, and out the door. The digital devices 88% of us carry (according to the Pew Internet pollsters) provide all sorts of things we used to depend on from other sources: newspapers, radio, brick-and-mortar stores, even (shudder) the U.S. Post Office.

Banking is no exception. FIS, the global bank technology provider reports its client base for mobile has increased more than 150% year-over-year, and that adoption by bank users or consumers of its mobile offerings has climbed more than 200% year-over-year. To put it in perspective, FIS says customers have used their smartphone cameras to deposit more than \$1 billion in checking accounts since the service was first offered not too long ago.

Related to this mobile mentality is the relatively new bring-your-own-device phenomenon, where employees of companies actually prefer using their privately-bought phones, tablets, and laptops for business purposes, rather than the hardware provided by their employers.

Gartner Inc., the business analyst, calls this phenomenon "the single most radical shift in the economics of client computing for business since PCs invaded the workplace."

"With the wide range of capabilities brought by mobile devices, and the myriad ways in which business processes are being reinvented as a result, we are entering a time of tremendous change," says David Willis, vice president and analyst at Gartner. "The market for mobile devices is booming and the basic device used in business compared to those used by consumers is converging. Simultaneously, advances in network performance allow the personal device to be married to powerful software that resides in the cloud."

BYOD, however, comes with a huge caveat, one that pervades the entire mobile ecosystem. That caveat comes down to one word: security. Companies, and even the users, are extremely nervous about having all their sensitive data at risk or even perceived as being at risk.

(For another perspective on the mobile security situation, read "Mitigating the risk in mobile banking" by Luke Nordlie and Hicham Chahine, Crowe Horwath LLC.)

Juniper Research estimates that the number of employee-owned smartphones and tablets used in the enterprise will more than double by 2014, reaching 350 million from almost 150 million this year. Still, its report found that the majority of employee's phones and smart devices did not have any form of security software loaded nor were company materials protected.

That Pew Internet report finds that 54% of users who generally tend to download apps, at least once have decided not to download a particular app because it required too much personal information. Another 30% actually uninstalled an app that was already on their cell phone because they learned it was collecting personal information that they didn't wish to share.

Accenting this theme, as bullish as Gartner is on the technology consumerization trend, even it points out the draconian measures companies need to take to try to keep it under control.

"Gartner believes that IT's best strategy to deal with the rise of BYOD is to address it with a combination of policy, software, infrastructure controls, and education in the near term; and with application management and appropriate cloud services in the longer term," it says in a recent report.

That's business in general, but what about banks?

The news here is promising, at least according to the Global Financial Services Industry Security Study just completed by Deloitte. Some of its conclusions include:

- Almost two thirds believe their information security function and business are engaged, meaning the business function of a given financial institution actively and regularly requests support by the information security function-i.e. cross-silo cooperation.
- More than half indicate they have a strong working relationship with operational risk management.
- Almost half claim to actively manage vulnerabilities, 82% of whom are also actively researching new threats to proactively protect their environment from emerging threats.
- Information security governance, identity and access management, and information security strategy and roadmap are cited to be the top security initiatives for this year.

Of course, there are problems as well. Respondents say a lack of sufficient budget (44%) and the increasing sophistication of threats (28%) are the primary barriers to implementing an effective information security program.

Drilling down just to the banking respondents (as opposed to the insurance company respondents), when it comes to adoption of mobile devices, respondents indicated that the top three security controls are: enhancing the consumer acceptable use policy; integrating consumer device security into awareness campaigns; and enforcing complex passwords.

It's a perplexing issue. It's not likely people will give up their gadgets en masse any time soon. It's more likely that even more seductive and addictive gadgets are soon to come along. Yet people still expect to be protected. Go figure.

One part of the solution is education. That's sort of a constant in all the talk about mobile, but still tends to lurk in the background. The thing is, there are all sorts of training courses available. ABA has long specialized in banking-specific programs in all sorts of formats-in person, online, over the phone. Conferences, schools, and meetings all provide relevant material related to mobile security. Check out the Training and Events page on www.aba.com.

Along these lines, Trustwave should be mentioned. The company is endorsed by ABA's Corporation for American Banking for information security and data protection. It just announced that it now provides cloud-based security education services that enable organizations to better equip their employees to protect against security risks and compliance missteps.

It's worth checking out. As its chief marketing officer, Leo Cole, says: "One of the most critical links in the security lifecycle is ensuring that employees are educated on security and compliance best practices."

##

Some of the sources for this article include:

FIS Drives 150 Percent Growth in Mobile Clients as Bank Customers Go Mobile in Record Numbers

Gartner Says Bring Your Own Device Programs Herald the Most Radical Shift in Enterprise Client Computing Since the Introduction of the PC

Press Release: Security Issues to Escalate as 350m Employees to Use Personal Mobile Devices at work by 2014

Privacy and Data Management on Mobile Devices

Trustwave Introduces New Security Education Services

About the Author John Ginovsky is contributing editor of ABA Banking Journal and editor of the publication's TechTopics e-newsletter. For more than two decades he has written about the commercial banking industry. In particular, he's specialized in the technological side of banking and how it relates to the actual business of banking. He previously was senior editor for Community Banker magazine (which merged with ABA Banking Journal) and was a staff writer for ABA's Bankers News. You can email him at jginovsky@sbpub.com