
Consider the headaches inherent in BYOD

By John Ginovsky

The trend dubbed "bring your own device," or BYOD, is emerging as a perplexing problem in the workplace, including banks. On the one hand, it seems it could be a benefit to the bank, since employees often have much more capable smart phones, tablets, and other gadgets than the bank can supply in a timely manner. On the other hand, though, the trend poses intense security problems when employees seek to access the bank's confidential systems with these devices, even when the employees do it with the best of intentions.

ABA Banking Journal Tech Topics talked about this issue with Nicholas Percoco, senior vice-president of Trustwave, a provider of information security and data loss protection that is endorsed by ABA's Corporation for American Banking.

Tech Topics: What are the security concerns regarding BYOD?

Nicholas Percoco: Allowing employees to bring their own devices does insert some security risks into the enterprise. What basically happens is a user goes into an electronics store and purchases a mobile device, anything they want. Or they get a device along with a contract with a wireless carrier. They bring it to their company and want to connect to the wireless network there and configure it to access email. What comes along with it are the inherent security risks within those consumer-level devices, right out of the box...What typically will happen is that users will have devices that they may or may not be able to get security patches for. Someone could get a device from a carrier that's on sale, or it's free with a signup for a plan. Then within a short period of time, a year or so, that device is no longer supported by the manufacturer. They no longer will get security patches for it. That becomes a real issue.

Tech Topics: There seems to be a positive side, though. It could be to a bank's benefit for an employee to use a sophisticated device to help do the job, without the bank paying for it. How do you balance the pros and cons?

Percoco: The pros—you have happy employees who are able to use the device they are used to, the device they like, for work purposes. On the flip side, as a security person within a bank, you now have to worry about all the security concerns on all the devices your employees now have. It becomes very, very difficult.

Tech Topics: So how could the IT department go about managing this?

Percoco: There is a hybrid approach where the bank will say, "You can bring your own device. You can purchase your own device. But it must be of this type of device. It must be able to support this version of [such and such]." They [the IT department] will put some parameters in place so it's not as extremely open as saying, "Bring any device you want," but they would allow employees to select from a handful of devices that have been preapproved by the IT security department. That's one way to get a handle on it.

Tech Topics: Any other suggestions?

Percoco: The other step a company will take is to allow users to purchase from a select list but also will have a policy that says, "If you are going to bring your own device you need to succumb to a mobile device management system that we as a company maintain on behalf of the organization." If they bring their own device, in order to connect to the corporate environment they now have to allow that device to come under the management of the IT security group. Where there are things like a major flaw that develops, the IT group could then know which devices in the organization are vulnerable to that particular kind of attack.

Tech Topics: What typically happens when the security department conveys to employees these security concerns?

Percoco: From an employee's standpoint, when a company says "If you want to use a device, I want to install device management on it to be able to see what the status of that device is," many times the employee's first reaction is that, "My company wants to be Big Brother and wants to know what I am doing." For the most part, that is not the case. It's basically those incidents of risk or compromise that take place. [Security people] want to be able to quickly query their population to understand who else is at risk.

Tech Topics: So it is a communications issue?

Percoco: If you send a notice every single time there's a mobile security risk to all employees, whether it applies to them or not, before long it becomes a broken record. Employees keep seeing these alerts coming from IT and they just start ignoring them. You want to be able to focus the attention, for any kind of security communication, on the people who it affects. Mobile device management and being able to query your population for their various risks becomes very important.

Tech Topics: Is this a growing issue?

Percoco: Certainly I think it is a growing issue…If you think about the job of the security person within a company, their job was difficult enough when they had to maintain the security of their own devices, and keeping track of software packages, and patches, and various things. Now you bring in the mix of anything you want to work, it grows exponentially.

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

[This article was posted on April 4, 2012, on the website of ABA Banking Journal, www.ababj.com, and is copyright 2012 by the American Bankers Association.]

