

BYOD grows up, intensifies

Love it, hate it, it doesn't matter. Management at the least has to learn to tolerate the consumerization of devices in the work place, and, at the best, create and enforce policies acceptable to all parties-IT managers, security managers, business managers, and employees themselves.

A slew of studies and white papers have appeared over the past few months, all of them saying one way or another that "bring your own device" is here to stay, is intensifying, and, as paradoxical as it may seem, bringing great savings and increased productivity on the one hand, while also producing intense problems on the other.

"The era of the PC has ended. Employees are becoming more mobile and looking for ways to still be connected wherever work needs to be done," says Phil Redman, research vice president at Gartner Inc. "The convenience and productivity gains that mobile devices bring are too tempting for most companies and their employees. Securing corporate data on mobile devices is a big challenge, but one that companies must embrace. Enterprises are struggling with how to support and secure this dynamic workforce."

Gartner predicts that over the next five years, 65% of enterprises will adopt a mobile device management solution for their employees.

Trend Micro commissioned a survey by Forrester Consulting this summer which found that across the United States and Europe, 78% of enterprise IT leaders say that employees are already using consumer devices to conduct company business. At the same time, another survey for Trend Micro found that device security is the top concern by management. It found that 83% of companies that do permit BYOD have policies in place that require employees to install security software as a precaution.

Which is where the paradox comes in. Of these companies that permit BYOD and allow employee-owned devices to connect to the company's network, 47 % have experienced a data breach. Of these enterprises, the immediate response was to impose data access restrictions (45%) or install security software (43%). Only 12% shut down BYOD altogether following a breach.

"Companies that are questioning whether or not to allow workers to bring personal devices into the workplace should just stop asking. It's clear that you can get a competitive edge when you put the right precautions in place," says Cesare Garlati, vice president of mobile security, Trend Micro.

Unisys Corp. weighed in with its own study, this one also conducted by Forrester Consulting, which concludes that "a super-connected class of mobile elite workers is defying IT policies to work more efficiently and serve customers, but potentially creating big risks along the way."

It defines the "mobile elite" as those individuals who make intensive use of multiple personally owned devices and applications to get work done. "In their zeal to be more productive and service-centric, mobile elite workers, whether intentionally or not, may be opening up new management, support, and security risks for their organization," Unisys says in its survey report. Such zeal can be seen in the finding that 82% of such workers have downloaded unauthorized applications to get work done, in spite of the fact that 75% of IT managers consider such practices as grounds for dismissal.

"Rather than fighting this trend, we believe CIOs and IT decision makers should study the behavior of these mobile elite workers in order to understand which approaches provide real innovation and differentiation for their organizations, and then craft their mobile infrastructures to safely support these activities," says Fred Dillman, Unisys chief technology officer.

Believe it or not, there's a flip side to BYOD concern-employees themselves are alarmed that their employers can track them through their personal devices 24/7, and can even collect personally identifiable information, find out which applications that they've installed, and review or delete personal pictures and music.

Fiberlink conducted a Harris survey and found many employees are unaware of such capabilities, unless they are specifically informed through an acceptable user agreement and mobile policy. It found that 82% of employees consider the ability to be tracked an invasion of their privacy, and 76% would not give their employer access to view what applications are installed.

"The survey results show that the vulnerability of personally identifiable information is a significant concern, and that organizations need to be just as concerned about user privacy as they are about the security of corporate data," says Christopher Clark, president at Fiberlink.

So what can be done about all this? Advice comes from several corners.

RSA, the security division of EMC, recently issued a research report from its Security for Business Innovation Council. It recommends five strategies for building effective, adaptable mobile programs:

- Establish mobile governance. Organizations should engage cross-functional teams to set clear ground rules.

- Create an action plan for the near term. Mobile security technologies are fast-moving and, in many cases, too nascent to allow long-term investments.

- Build core competencies in mobile app security. Design mobile apps in a way that protects corporate data, not just by bolting on security, but by examining the app's overall functionality and architecture.

- Integrate mobility into long-term vision. Include risk-based, adaptive authentication, network segmentation, data-centric security controls, and cloud-based gateways.

- Expand mobile situational awareness. Corporate security teams should deepen and continually refresh their understanding of the mobile ecosystem.

Fiberlink, which offers the maas360 mobile device management solution, takes another approach to BYOD advice, proclaiming the "Ten Commandments of BYOD." Briefly, they are:

- Create thy policy before procuring technology.

- Seek the flocks' devices.

- Enrollment shall be simple.

- Thou shalt configure devices over the air.

- Thy users demand self-service.

- Hold sacred personal information.

- Part the seas of corporate and personal data.

- Monitor thy flock-herd automatically.

- Manage thy data usage.

- Drink from the fountain of ROI.

(Check the link below for further explanations of each of these points.)

The message is clear that businesses need to deal with BYOD now and for the foreseeable future. Back to Gartner:

"This is just the start for [mobile device management]. More data is being put on mobile devices, and enterprises are fast developing their own applications to support their mobile users. As mobile devices continue to displace traditional PCs, enterprises will look to their existing MDM systems to support more devices and enterprise applications and data," says Redman. "MDM vendors are moving beyond security, to support enterprise and third-party applications, data, and content. In the next two years, we will continue to see MDM platforms broaden out and become more enterprise mobile system management platforms, not just for devices alone."

##

Sources used in this article include:

Gartner Says Two-Thirds of Enterprises Will Adopt a Mobile Device Management Solution for Corporate Liable Users Through 2017

Harris Survey Exposes Concerns About Employee Privacy for BYOD

New RSA Research Tackles Mounting Risks from Mobile Devices in the Enterprise

The Ten Commandments of BYOD

Consumerization is Here: Surveys from Trend Micro Confirm that BYOD is Overtaking the Workplace and That Device Security is Top Concern

The Great Divide: Mobile Workers Challenge IT Departments with Aggressive Use of Consumer Tech, Unisys-Commissioned Study Finds

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