From: www.cio.com

How IT Can Scare Off BYOD Monsters in the Closet

– David Taber, CIO

August 08, 2013

BYOD is a reality, and we all have to deal with it.

Most of us are used to well-behaved devices such as laptops, netbooks, iPhones and iPads. There are enough mobile device management products to handle remote wipes and other strategies to lock down these devices if they are lost or stolen.

But when the device doesn't have a disk, things get a little dicey. Flash RAM that's soldered into a device can't be removed practically, and if the device is broken, that memory can't be erased. It gets more fun with Android tablets; the hardware may not be all that long-lived, and the myriad software configurations can be hard to manage in the wild.

Guides: All About BYOD and 12 BYOD Disaster Scenarios

Now, let's assume that the user's device dies or becomes otherwise unreliable. The malfunctioning device is often put in the back of a drawer at the office or into a closet at home with a bunch of other stuff that's out of sight, out of mind and soon forgotten.

This is the genesis of IT monsters in the closet.

Months later, somebody has the great idea to clean out the closet and get rid of all those old games, cameras, phones and Android devices that flaked out (typically due to a broken connector, cracked screen or weak battery). Off they go to eBay, Craigslist or somebody's favorite charity.

Now the monsters have been let loose—probably with some of your corporate data or passwords still in memory. But nobody will remember what's in there; it's been months since the devices could even boot.

There's a chance the device can never be revived and your data is therefore safe. But in a recent episode, one of our clients was not so lucky. An enterprising eBay purchaser cracked open the case of the dead device, replaced a defective connector and, within minutes, had access the former owner's corporate and personal confidential information. Since the device was never brought onto the network, the flimsy auto-destruct sequences could never kick in.

Research: Most BYOD Businesses Exposing Data to Cyber Criminals
More: Mobile Boom Turns BYOD Into Unmanaged Risk, Check Point Finds

Thankfully, identity theft and breaches didn't happen—but that's only because the purchaser was a nice guy. He even had the decency to contact the client, notify it of the breach and wipe the data.

Avert BYOD Disasters With Advanced Planning

A mobile security policy shouldn't depend on good luck. What, then, *can* you do? Here are seven suggestions.

Case Study: VMware Going 'All In' with BYOD

- Encrypt and password-protect data on the device, any place you can. Of course, single sign-on on most mobile programs is a slim-to-none proposition, so user patience is a constraint here.
- Require passwords on every sign-in, if you can. But know that, with some effort, these policies can typically be bypassed on mobile devices.
- Of course, use the latest information leakage prevention (ILP) and data loss prevention (DLP) tools you can find. Same goes for auto-erase and call-home software on the device.
- Somehow, though, you have to get users to install and update these things on their devices. Make your network security mechanisms enforce this. Once the device is registered on the network, the device owner should be contacted via phone if the device has been off the air for more than a month (to make sure that it's not living in a closet somewhere). For large, sophisticated companies, this is all an "of course" proposition—but for most SMBs and small office home office (SOHO) operations, it's an "uh-oh."
- Establish a corporate BYOD policy that allows devices on the network only if the owner agrees that they will never be given away, sold or recycled. Instead, the company will purchase them at a nominal value so that they can be fully wiped (or, worst case, destroyed) before going off to charity/recycling.
- Also establish a hotline for reporting lost or stolen devices and develop a protocol for locking down data and changing passwords on accounts inside and outside your network. Again, this is standard stuff for big companies but an "uh-oh" for smaller ones.

- Finally, set up a BYOD FAQ that employees must at least glance at before their device is allowed to connect to any corporate data assets. This FAQ should have a login/click-through sequence (similar to a license agreement) that confirms they've at least skimmed it.

Analysis: Are Businesses Rushing to BYOD Too Quickly?
More: The 3 Extremes of Corporate BYOD Policies

Of course, procedures and add-on software like this all cost money, making that "free" device the user pays for a costly little item indeed. This is what economists call an "externality," as it causes downside and risk for people who *aren't* making a decision.

If you really think it through, it may be cheaper for your company to provide Android devices—all with known configurations and identical hardware—instead of letting users bring their own.

Ah, the price of "free."

David Taber is the author of the Prentice Hall book, "Salesforce.com Secrets of Success" and is the CEO of SalesLogistix, a certified Salesforce.com consultancy focused on business process improvement through use of CRM systems. SalesLogistix clients are in North America, Europe, Israel and India. Taber has more than 25 years of experience in high tech, including 10 years at the VP level or above.

Follow everything from CIO.com on Twitter @CIOonline, Facebook, Google + and LinkedIn.