COMPUTERWORLD

Print Article ⊠ Close Window

Security Manager's Journal: Security is left out of another decision till too late

Replacing the printers with machines that can do a whole lot more must have seemed like a no-brainer. In reality, not quite.

J.F. Rice

September 21, 2009 (Computerworld)

Do you know what gets old really fast for a security manager? It's being told that some decision has been made, that it's too late to modify it, that no one thought input from the security manager was needed, and that there's no budget to deal with the concerns he's raising at the eleventh hour. All of this has just happened to me -- again.

This time, the problem is MFDs -- multifunction devices that look like photocopiers on steroids. I found out that we had signed a contract to replace all of our printers with MFDs when workers showed up to haul away all our laser printers and then started wheeling in these new monstrosities.

I thought our old printers were fine, but apparently we can save a lot of money by using these new "smart" devices that can call for help when they run out of paper, need toner or get jammed. They are all network-connected and can print, scan, copy, fax, e-mail and do just about everything except the dishes. Sounds cool, right?

Trouble Ticket

At issue: Company printers have been replaced by multifunction devices that have brains -- internal Windows computers.

Action plan: Find a way to get these new computers updated regularly, for starters.

The problem is that they aren't really printers. They are network-connected computers with attached peripherals to perform numerous functions. I talked with the vendor and found out that these MFDs actually run Windows -- and a very old version at that. Suddenly, we've introduced a bunch of new Windows machines to our network. You might recall that I've expended significant effort this past year to get a handle on Windows patch management. These new devices change the equation.

I met with the project manager to learn more about what's going on and determine how to get some security controls and practices into the work plan. She wasn't very pleased to see me. "These are just printers," she told me. "Why do we need to worry about security?"

Now, there's a question that'll get you on my good side. In response, I switched to education mode. I explained how the "brain" of these devices is really a Windows computer, and therefore we would want to harden them according to our standards and find a way to update their underlying software every month, as well as lock them down. This was not a welcome revelation. "We don't have budget for that, nor do we have the time," she told me.

Define 'Temporary'

The MFDs were all rolled out within two days, and now they are hulking security exposures on our network, just waiting for a worm or virus to come along. But there are other concerns. Here's the most worrisome one: Any document that is scanned, printed or e-mailed on an MFD will be stored "temporarily" on the machine's internal hard drive. I put the word *temporarily* in quotes because those files will stick around until the system deletes them to reclaim space. Worse, should a machine fail, our vendor will come out and take it away and replace it -- and who knows where those "temporary" document files will end up? Oh, and that replacement MFD will have to be hardened, assuming we ever manage to do that with the ones that just arrived.

I have to figure out how to lock these things down, and how to keep them updated. If I had been in the loop before the contract was signed, I could have argued for at least signing up for quarterly updates via CD. That would have added expense, it's true, but contracts shouldn't be signed on the basis of saving money -- especially when no real effort has been made to find out about all of the costs that will be involved.

Ironically, my company has a pretty good process for reviewing the security of new technologies. But for that process to work, people have to recognize that certain devices we buy *are* new technologies. When they think of them as appliances, the security element gets kicked to the gutter.

This week's journal is written by a real security manager, ***"J.F. Rice,"*** *whose name and employer have been disguised for obvious reasons. Contact him at jf.rice@engineer.com.*

Join in

To join in the discussions about security, go to computerworld.com/blogs/security