

Managing Consumer Tech in the Enterprise

By Wayne Rash

3 August 2010

eWeek

1. Managing Consumer Tech in the Enterprise

You've seen it happen dozens of times. One of your [business](#) buddies shows up with the latest gadget from the Best Buy ad over the weekend, and now he wants to use it at work. It might be a new smartphone, an external hard disk or even a personal wireless access point, but whatever it is, it's not something that has been approved to work in your business.

Normally you wouldn't care, but as an [IT administrator](#), you have to listen to your buddy gripe about how awful it is that the evil network folks won't let him just plug and play. Surely there's a way around this, right? The answer, of course, is maybe.

The secret to living with the inexorable incursion of consumer technology is to embrace what's good, control what's risky and educate people about those things that really are unsuitable for use in the office. But it's important to know that most companies can benefit from the innovations in consumer electronics as long as you're prepared.

Being prepared can mean a lot of things when it comes to allowing consumer technology to exist within your company. In addition to education, it can mean adopting the right policies so the technology can be integrated safely, and it can mean not sticking with outmoded practices that effectively drive your employees to use their own consumer products instead of what you provide for the enterprise.

Personal e-mail use by employees is an excellent example. Many, perhaps most, enterprises have a limit on the size of e-mail attachments. Often this is in place to prevent your e-mail server from filling up with too much clutter. But there's another side to this issue. If you don't make it possible for your employees to send large files to each other when their work demands it, then you're effectively giving them no option but to go outside of the enterprise, and incidentally outside of the security and audit trail that goes with it.

The easy solution is raise your e-mail attachment limit to something that will at least allow a PowerPoint [presentation](#) to be sent from one office to another. You should also probably provide some means of sending larger files with programs such as [YouSendIt](#) or [Accellion managed file transfer products](#). "Organizations should be thinking about how they should outfit their employees with file transfer," said Accellion Chief Marketing Officer Paula Skokowski. "Employees would not be looking at work-arounds if the company provided them."

The same is true for other employee-provided technology for getting their jobs done. Handled right, it can be a benefit to the company. "I always thought it was nuts that if someone was willing to spend their own money to help them do their job better, that you wouldn't embrace it," said Doug Neal, research fellow for the Leading Edge Forum Executive Program. Neal said companies need to have a different attitude toward employee-owned gadgets since, in the long run, it will probably be impossible to keep them out of the workplace. He suggests engaging employees in the solution, and helping them use their personal devices to improve their productivity where possible. "We're creating security problems if we don't adapt in the way we should," Neal said.

But of course that doesn't mean you can just throw open the doors and let any employee bring in anything at all. You're still responsible for security and compliance, so you have to make sure that whatever devices you allow to handle sensitive data comply with security requirements, and that their use is auditable. It also means that you need to have policies about how such devices are used, and how to enforce those policies.

In general, it's important to either provide the products employees need or help employees control the devices they bring to work. In many companies this has become a necessity as many have moved to allowing or requiring employees to provide their own smartphones and laptop computers. If you're requiring that employees have the devices, then you need to also make sure that they can handle them responsibly.

Edy Almer, vice president of product management and marketing at Safend, pointed out that helping employees do the right thing is the only sensible course of action anyway. Almer said he's seen any number of efforts by companies to block access to USB ports, or to block large file transfers, but he said such efforts are ultimately doomed. "The users will find a way," Almer said. Worse, the result could be uncontrolled and unmonitored connections to the outside world. "You can end up with multiple connections into the organization," he said.

Almer suggested the use of software (such as that made by Safend) to encrypt any data that goes out a USB port so that there's no danger of a data breach if someone loses a memory stick, and to monitor where the data goes for compliance purposes. He also suggested that other things that drive security officers nuts, such as social networking and personal e-mail, aren't really that big a problem. "You can't block them completely," Almer said.

"You're better off allowing it but having a policy in place and monitoring transfers. If you're blocking users, they're savvy," he said, pointing out that they'll just find a way around your blocks. "You're better off allowing them to do what they want, and letting them know what's allowed."

2. Understand What's Being Used and Why

However, it's also important to know why employees are bringing their gadgets to work. "When they're using consumer products during the day, why are they doing it?" asked Lori Wizdo, vice president of marketing at Knoa Software.

Wizdo cited as an example a company that created a knowledge base for its call center. "Agents would open the call center application knowledge base every day, but not use it," she said. "They went to the Internet instead."

Wizdo said the agents found that using an Internet search engine was easier and faster than using the knowledge base, so the company eliminated it. "They were able to understand what the agents were actually doing."

Using consumer electronics and other consumer products may mean that you're not providing the right tools to your users. "End users will seek out and find best solution," Wizdo said. "If all of the [sales](#) force is starting to use Hotmail, instead of the company e-mail system, it's a symptom of a problem," Wizdo said. "There's something wrong or inadequate about the tools you're giving the company."

According to Wizdo, one of the best ways to get a handle on how employees use consumer products is to [monitor](#) what they're doing. Wizdo said monitoring tools, such as those provided by her company, can give an important look into why employees aren't using the enterprise tools you gave them and instead are using products they bought themselves. "Are the end users using the tools you've given them to do the job?" Wizdo asked. "Are they using a different set that they've self-selected? What are the choices the employees have made? Do they have risks or costs, or should they be made best practice?"

In many cases, Wizdo said, employees bring their own tools to work because the ones selected by the company don't work well, or they may not work at all. "Why aren't they using the tools? Am I not using Outlook Web Mail because it takes 10 times as long as Hotmail? Can I remediate it? Is it creating behaviors you don't want? Are the end users using the technology well? Are they making errors,

stumbling through?" Wizdo said the answers to these questions can tell a company whether it's made the right choices in the tools it provides, and whether the tools are working as they should.

But Wizdo also said companies should think twice before banning all such employee-provided solutions. "If you shut it all down, then you're shutting down innovation, too," she said. Wizdo pointed out that in many cases consumer tools are far ahead of their enterprise counterparts in terms of innovation. She suggested that with proper monitoring and controls, companies can benefit two ways: by letting employees pick up the costs of the tools they need, and by benefiting from the innovation they bring.

Neal of the Leading Edge Forum Executive Program suggested that rather than fighting against consumer technology, companies find a way to embrace it, and a way for employees to participate in making the new technologies work within the organization. He contended that companies need to work with employees to reach agreement on how new technology should be handled. To do this, he recommends two rules:

1. Don't embarrass the company
2. Your responsibility for data does not end; you have to make sure it doesn't get harmed.

"People are going to figure out how to do their job," Neal said. "They'll either do it with you or without you." He added that getting people to understand their responsibility for the company's information and getting their agreement to protect it will go a long way to easing the problems created by consumer technology.

Of course, that doesn't mean not having controls. You still need to insist that mobile devices can be wiped if lost, that data loaded on portable and mobile devices is encrypted and that you will monitor what is copied to those devices so you can maintain their compliance status. But rather than forcibly limiting what people can do with their personal devices, it makes a lot more sense to make it possible for people to incorporate the devices they want to use into their daily work lives. It saves the company [money](#) and, if done right, it won't hurt security

3. People Will Find a Way to Do Their Jobs

According to Alan Brill, senior managing director of [Computer Forensics](#) at Kroll Ontrack, a company's management can make a big difference in how employees use their personal devices at that company. Often the biggest problem, Brill said, is that the IT department doesn't have the budget to buy the products or services that employees need to do their jobs, so they do so themselves.

"If somebody can't get their job done because they can't get something they need, and their boss turns them down, and you force them to go to Plan B, how much can you blame them for doing that?" he asked.

Brill said much of the reason for the budgetary lack is because upper management doesn't understand the work that their employees do, and doesn't understand why they need these devices to help them do it. The solution, he said, is to get the attention of senior management so that they understand why employees need these products or services. "When you move to potential civil liability and regulatory failures, you're not going to cause senior management's eyes glaze over," he said.

Brill noted that it's critical to get management buy-in on moving to new technology.

He also recommended adopting a proactive look at the potential security issues that created by bringing consumer electronics into the workplace. He suggests:

- Have a policy. Establish a set of rules and let people know what they are. You can't go after someone for doing something they didn't know they shouldn't.
- Have tools to enforce those rules. You have to have controls.
- Company IT people have to be aware of legal implications of their actions.
- Question potential violations—ask, Why is that iPhone connected?
- Add an item to annual [performance](#) reviews on whether employees are doing the right thing to protect information.

Brill said it's really better to get employees to help control data loss than to take some of the measures he's seen. "I've walked into some places and seen somebody trying to squeeze a tube of Superglue glue into a USB port to prevent its use," he said.