

Active Blog
Managing

www.active-technologies.com
info@active-technologies.com

Consumer Technologies – Ban Them All Or Let Them Slide

It's a fact that high-tech consumer products and services of all kinds are making their way into the workplace. They include everything from smart phones, voice-over-IP systems and flash memory sticks to virtual online worlds. And as people grow more accustomed to having their own personal technology at their beck 'n' call -- and in fact can't imagine functioning without it -- the line between what they use for work and what they use for recreation is blurring.

However, some of these consumer technologies can pose real security threats to your business. To help you decide on what consumer technologies to ban and what to let slide, let's take a look at eight popular consumer technologies and services that have crept into the workplace.

1. Instant messaging

People use instant messaging for everything from making sure their kids have a ride home from practice to communicating with co-workers and business partners. In the Yankee study, 40% of respondents said they use consumer IM technology at work. Instant messaging presents numerous security challenges. Among other things, malware can enter a corporate network through external IM clients and IM users can send sensitive company data across insecure networks.

One way to combat threats is to phase out consumer IM services and use an internal IM server. In late 2005, Global Crossing did just that when it deployed Microsoft Corp.'s Live Communications Server (LCS). Then in August 2006 it blocked employees from directly using external IM services from providers such as AOL, MSN and Yahoo. Now, all internal IM exchanges are encrypted, and external IM exchanges are protected, as they're funneled through the LCS server and Microsoft's public IM cloud.

Adopting an internal IM server also gave Global Crossing's security team more control. "Through the public IM cloud, we're able to make certain choices as to how restrictive or open we are. We can block file transfers, limit the information leaving our network or restrict URLs coming in," which was a common method for propagating worms, Miller says. "That takes away a huge component of malicious activity."

You can also take a harder line. DeKalb's security policy, for instance, bans IM use altogether. "It's mainly chat-type traffic, not personal health information, but it's still a concern," Finney says. As backup to the restrictive policy, she blocks most sites where IM clients can be downloaded, although she can't block MSN, AOL or Yahoo because many physicians use those sites for e-mail accounts. Her team also uses a network inventory tool that can detect IM clients on employee PCs. If one is found, the employee is reminded of DeKalb's no-IM policy and notified that the IM client will be removed. Finney is also considering various methods of blocking outbound IM traffic, but for now, she also uses a data loss prevention tool from Vericept Corp. to monitor IM traffic and alert the security team about any serious breaches. To do that, Finney's team needs to shut down most of its Internet ports, which forces IM traffic to scroll to Port 80 for monitoring.

DeKalb is looking into the idea of implementing the IM add-on of IBM's Lotus Notes or even an internal freeware IM service like Jabber for business users who want to communicate across campus. "Nothing is 100%," Finney says. "IM is always a huge concern from a security as well as a productivity perspective."

Active Blog
Managing

www.active-technologies.com
info@active-technologies.com

2. Web mail

Of the respondents to the Yankee Group survey, 50% said they use consumer e-mail applications for business purposes. The problem with consumer e-mail services such as those from Google, Microsoft, AOL and Yahoo is that the users themselves don't realize how insecure their e-mail exchanges are because messages are transported over the Web and stored on the ISP's server as well as the e-mail provider's server. Without that awareness, many use no discretion about sending sensitive information such as Social Security numbers, passwords, confidential business data or trade secrets.

One approach to tightening security around Web mail is to use a tool that monitors e-mail content using keyword filters and other detection techniques and the either generates alerts regarding potential breaches or simply blocks the e-mail from being sent. For instance, WebEx Communications is considering expanding its use of a data loss prevention tool from Reconnex Inc. to include e-mail monitoring, according to Michael Machado, director of IT infrastructure.

For its part, DeKalb addresses this problem with Vericept's tool, which captures a screenshot of every Web-based e-mail that employees send, including file attachments, and scans these for company-defined sensitive data, such as Social Security numbers. Alerts are sent to Finney's team so that they can follow up with users to educate them on the dangers of sending sensitive data over the Web.

3. Portable storage devices

One of an IT manager's biggest fears, according to Holbrook, is the steady proliferation in types of portable storage, ranging from Apple iPhones and iPods to flash memory devices. "People can use these to download any number of corporate secrets or sensitive information and move it off-site, which is not where IT wants that information to be," he says.

"In the past three weeks alone, I've heard six different conversations about the risks of flash drives and portable storage devices," says Mark Rhodes-Ousley, an information security architect and author of *Network Security: The Complete Reference* (McGraw-Hill Osborne Media, 2003).

While it would be easy enough to lock down the USB ports on employee PCs, many security managers say this is not a recommended approach. "If people want to subvert the process, they're going to find a way to get around any barriers you put in place," Miller says. "And where do you draw the line? If you restrict USB ports and [cell] phones coming into the office that may have data storage ports, then you have to look at restricting infrared ports on devices and CD burners, and the list goes on and on."

It's better, he says, to handle the matter by educating people on how to treat the storage of sensitive information. "Most of the incidents that occur are unintentional [rather than] malicious, so that's where education comes in, as to proper handling and why it's important," Miller says.

Machado says he isn't a fan of blocking USB ports at WebEx, mainly because such a strategy would quickly devolve into users asking IT for exceptions to the rule and IT having to manage those exceptions. "Everyone has an exception that they think is important, which takes up more of IT's time than is necessary," he says.

Active Blog
Managing

www.active-technologies.com
info@active-technologies.com

What would be optimal, he adds, is to have a tool that sends an to people who are trying to copy files to USB drives or other unencrypted storage media, advising them that they're going against corporate policy. "Then they know they're empowered to make the decision but that it's going to be tracked and monitored," he says.

On the other hand, DeKalb's Finney says she is interested in blocking technologies and is looking into the Vericept tool's ability to either block certain types of data from being transferred to an external storage device or alert her when someone tries to plug anything into a PC that's not native to that computer. Ideally, she'd like a tool that would also remind employees that corporate policy forbids sensitive data to be stored on external devices.

Meanwhile, Michigan's Grand Valley State University and other colleges and universities where professors and students have lost flash drives with sensitive data are looking into standardizing on password- and encryption-protected USB drives to protect them in the future.

4. PDAs and smart phones

More and more employees are showing up at work with some form of smart phone or personal digital assistant, be it a BlackBerry, a Treo or an iPhone. But when they try to synch up their device's calendar or e-mail application with their own PC, it can cause problems ranging from application glitches to the blue screen of death. "Those types of problems are not uncommon -- it's the mundane things like that that can drive IT nuts," Holbrook says. "It's not how they want to be spending their time."

Moreover, should the employee quit or be fired, he can walk out the door with any information he wants, as long as the PDA or smart phone belongs to him.

Like some other companies, WebEx minimizes those possibilities by standardizing on a single brand and model of PDA and letting employees know the IT organization will only support that one device. WebEx does the same thing with laptops, which Machado notes, represent an even greater threat than PDAs because they can hold even more data. Any unapproved devices are not allowed on the WebEx network.

5. Camera phones

A hospital worker stands at a nursing station, casually chatting with the nurses. No one notices she's got a small device in her hand, on which, from time to time, she's pressing a small button. A scene from the latest spy thriller? No, a security test conducted by DeKalb's Finney.

"One of the tests I did was to go to take my cell phone to the nursing station and start clicking off photos, unbeknownst to them," she says. "I wanted to download the photos, enhance the images and see what I got -- patient information displayed on computer screens or on papers lying on the desk."

As it turns out, she didn't obtain any personally identifiable information, but she did glean the computer name (not the IP address) from the top of the photographed computer screen.

"That kind of information can add up to clues that can be compiled or combined with other information someone could get from other sources in the facility to build a plan of attack," she says.

Active Blog
Managing

www.active-technologies.com
info@active-technologies.com

As a follow-up, Finney added information regarding this potential security breach to DeKalb's employee orientation and security awareness programs, so people are at least aware of how risky it is to expose sensitive data for others to see -- and possibly photograph.

6. Skype and other consumer VoIP services

Another fast-growing consumer technology is Skype, a downloadable software-based service that allows users to make free Internet phone calls. In fact, 20% of the respondents to the Yankee Group study said they use Skype for business purposes.

In a business setting, the threat presented by Skype and similar services is the same as that of any consumer software downloaded to a corporate PC, Holbrook says. "Enterprise applications are highly scalable and highly secure, while consumer applications are less scalable and less secure," he says. "So anytime you download Skype or anything else, you're introducing a security risk that IT is uncomfortable with." For instance, the software can interact with every other application on the PC or network, potentially affecting the performance of every application.

Skype itself has issued at least four bulletins announcing security holes that users can patch when they download the latest version of the software. But because IT often has no idea how many users have installed Skype, let alone who has done it, there's no way for them to police these efforts.

The most secure option, and one that research firm Gartner Inc. recommends, is to block Skype traffic altogether. If a business chooses not to do that, it should actively engage in version control of Skype clients using configuration management tools and ensure that it is distributed only to authorized users, Gartner says.

7. Downloadable widgets

According to Yankee Group, consumers are using devices such as the Q and the Nokia E62 to download widgets that give them quick access to Web applications. These widgets can be easily moved to PCs, which, according to Holbrook, represent another entry point into the technology ecosystem that IT struggles to control.

The risk here is that these tiny programs use processing power on the PC and the network. And beyond that, any software that gets downloaded without being vetted represents a potential threat. "It's not more likely to be infected with a virus, but you're downloading something you might not have a lot of trust in," Holbrook says.

WebEx mitigates this risk using a threefold approach. It educates users on the risks of software downloads; it uses Reconnex to monitor what's installed on user PCs; and it disables some of the users' default access rights, restricting their download capabilities.

8. Virtual worlds

Business users are beginning to experiment with virtual worlds such as Second Life, and as they do, IT needs to become more aware of the accompanying security concerns. It would be short-sighted, Holbrook says, to simply block the use of these virtual worlds. "It's an application that people are just now figuring out how it can be useful in a business setting," he says.



Active Technologies, LLC

(843) 225-5648

Active Blog
Managing

www.active-technologies.com
info@active-technologies.com

At the same time, using Second Life involves downloading a large amount of executable code and putting it inside the corporate firewall, Gartner points out in a recent report. In addition, there's really no way to know the actual identities of the avatars who populate the virtual world.

One option that Gartner suggests is enabling employees to access their virtual worlds over the company's public wireless network or encourage them to do it from home. A third option is for companies to evaluate tools to create their own virtual environments that would be hosted internally within the enterprise firewall.

If you require additional information or assistance with this item, please give us a call.