Network security has focused on building impenetrable outer walls, but IT managers might take a lesson from history and protect their more vulnerable openings: the ports on their PCs.

Michael Thelander

The Great Wall Syndrome

In 1644, a man named Wu Sangui opened a gate. His act might never have caught history's attention were it not for the peculiar significance of time and place: Wu Sangui was a general for China's ruling Ming Dynasty, the gate was in China's Great Wall at Shanhai Pass, and on the other side of the gate was the invading Manchu army. An inside job defeated the greatest fortification ever known to man—begun in the second century BC, expanded and strengthened over generations, and perfected by the Ming from 1368 to 1620. Within a year of Wu Sangui's act, the Manchurian invaders had overthrown the Ming and established the Qing Dynasty, which ruled China for the next 300 years.

This historical detour might have implications for corporate security, IT infrastructure, and the easy access to technology we enjoy today. As was the case in 1644, IT organizations generally perceive their greatest threat to be faceless dangers on the outside, although real and immediate dangers often exist inside as well. While the Mings were fortifying their wall against the Manchurians, discontent and disillusionment were building within.

A 2004 survey of Fortune 100 companies by the Ponemon Institute found that insiders were responsible for roughly 70 percent of reported security breaches (Marguerite Reardon, "Securing Data from the Threat Within," *CNet News*, 12 Jan. 2005). BBC News, quoting another recent survey by data forensics firm Ibas, stated that 70 percent of staff surveyed have stolen key information from the workplace, that 72 percent of these offenders had no ethical issues with helping themselves to information that would benefit them in a new job, and that 30 percent of respondents had stolen contact data when they left an employer ("Workplace Data Theft Runs Rampant," *BBC News Online*, 15 Feb. 2004).

These attitudes toward corporate security are not new. What is perhaps new is the unprecedented ease with which individuals can carry away huge amounts of previously unmanageable digital property. Every organization has a main gate, represented by firewalls, decentralization, and change control systems. But we might be well-served to think of every computer's set of Universal Serial Bus and FireWire ports as inviting side doors, and of the growing army of PDAs, USB drives, and media players as Trojan horses that can siphon intellectual property through these doors at surprising rates. Where would-be thieves might think twice about sending a traceable e-mail containing data to an external destination, or carefully consider the risk of burning an entire directory of engineering documents to their local DVD drive, such "lifestyle devices" seem to suspend the threat of discovery. A seemingly innocent flick of the mouse can, in a fraction of a second, copy files of business-altering significance to a PDA, iPod, or memory stick that an employee casually plugs and unplugs every day. (See also the "Who Should Care the Most?" sidebar.)

THE THREAT OF LIFESTYLE COMPUTING

"Lifestyle computing" has become a catchphrase for the application of advanced computer technology to mass-marketed consumer devices. A

Inside

Who Should Care the Most?

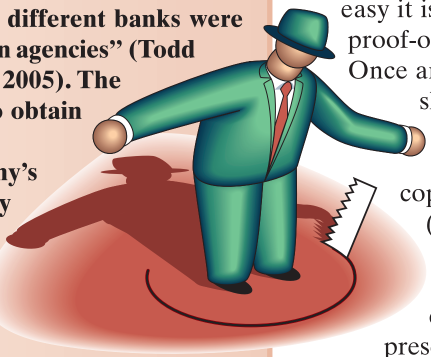
Products of Further Interest

1520-9202/05/$20.00 © 2005 IEEE

Who Should Care the Most?

The threat represented by lifestyle devices is both industry- and sector-agnostic, but certain high-risk groups may find themselves particularly vulnerable:

- ***Finance.*** **A May 2005 *ComputerWorld* article described a scheme in which "electronic account records for some 500,000 banking customers at four different banks were allegedly stolen and sold to collection agencies" (Todd R. Weiss, *ComputerWorld*, 18 May 2005). The ringleader hired bank employees to obtain the records.**
- ***Technology.*** **A technology company's primary assets—intellectual property and product plans—are painfully small and transportable. At the same time, these companies often foster a culture that urges the adoption of new gadgets and tools.**
- ***Government.*** **Many military installations ban MP3 players and portable storage devices from sensitive areas as protection not only from data theft but also against malware and other virus threats. Other branches of government have taken similar steps, but as these devices' popularity evolves into ubiquity, organizations will find that bans are more difficult to manage and will seek a control mechanism.**



phenomenon of both technology and marketing, Apple's iPod is an example of this trend: a tiny storage device that can hold up to 60 gigabytes of data accessible through lightning-fast input and output speeds, doubling as an entertainment device. In essence, the iPod is a walking hard drive that fits in a person's palm and can talk through USB and FireWire protocols to either Windows- or Apple-based operating systems.

Many other examples exist. USB pen drives can hold 8 Gbytes of data, and memory sticks are so commonplace that corporations use them as marketing vehicles, adding their brand names and logos. US-based Archos has introduced a 100-Gbyte handheld digital video recorder. Storage device leader Seagate recently introduced a yo-yo-sized 5-Gbyte portable hard drive, as well as an 8-Gbyte flash RAM card for digital cameras that can store files of varying formats and types. Without too much undue paranoia, you could read "smaller" and "more powerful" as "easier to hide and manipulate" and "capable of making a bigger digital haul."

A 2004 Gartner Group research report warned of the threat represented by the accessibility, ease of use, and portability of lifestyle computing devices. These devices "present risks to businesses on several fronts: from introducing malicious code into a corporate network, to being used to steal corporate data" (Ruggero Contu, *How to Tackle the Threat From Portable Storage Devices*, Gartner Group, July 2004).

Britain-based *New Scientist* magazine published an article in July 2005 showing how easily this abstract threat could become corporate reality. "Abe Usher of security consultancy Sharp Ideas in Centreville, Virginia, has shown just how easy it is to pod-slurp, as he calls it, with a proof-of-concept program called slurp.exe. Once an iPod is plugged into a computer, slurp.exe takes just 65 seconds to rifle through its hard drive, home in on all Excel, PDF, and Word files, and copy them to the iPod hard drive" ("Beware of Strangers Bearing iPods," *New Scientist*, June 2005).

Beyond the deliberate theft of digital property, these devices also present a serious virus risk. PDAs, iPods, and microdrives migrate effortlessly between typically secure work environments and typically nonsecure home environments. An October 2004 National Cyber Security Alliance (NCSA) study showed that 67 percent of all home PCs have no firewall protection whatsoever. Of the survey's respondents, 63 percent reported that they had experienced viruses on their home PCs, and 50 percent "didn't know" whether they currently had a virus. Remote scans showed that 19 percent of the surveyed PCs were infected with a worm or virus at the time of the study, even though 70 percent of these users believed they were protected against viruses and intrusion (*AOL/NCSA Online Safety Study*, America Online and the NCSA, Oct. 2004, http://www.staysafeonline.info/news/safety_study_v04.pdf). The lifestyle devices that shuttle between the home and corporate worlds are likely serving as effective virus carriers.

Despite these threats, few organizations could go so far as to adopt the Gartner report's ultimate suggestion, "these devices should be banned from corporate environments," without making significant changes. The tide of cultural acceptance for these devices has carried them into every level and region of modern society, and ungoverned bans are likely to meet stiff resistance. Any ban would likely create a sort of "iPod underground movement" that would foster creative and security-threatening work-arounds for bringing devices into the workplace and connecting them to the network. What is needed, instead, is the understanding that this is a long-term IT management issue that will require a long-term, two-tiered approach to solving the problem:

1. Organizations will need a robust, well-defined, and broadly communicated acceptable use policy (AUP) for

both corporate and personal devices.

2. A solution will require network-based management tools that can monitor and enforce the established policies and can be effortlessly deployed.

THE ACCEPTABLE USE POLICY REVISITED

Most organizations, especially those in technology and government, have already established AUPs to oversee the use of technology equipment, software, and services. AUPs typically specify what is permissible and what is not permissible in an organization's IT environment. The policy should leave no doubt as to what employees should expect when they are on the network, and should spell out the consequences if an associate, staff member, or employee fails to comply.

Table 1. Authorized Users for Various Device Types.

Users	Media players (iPod)	Hard drives and memory sticks	Digital cameras and recorders	CD and DVD recording
General users	No	No	No	No
Department managers	No	Yes	No	No
Field sales	No	Yes	No	No
Finance	No	No	No	No
IT administration	No	Yes	No	Yes
Marketing	No	No	Yes	Yes
R&D engineers	No	Yes	Yes	Yes

As a first step toward corralling the security risks that lifestyle devices can pose, an organization should update its policies to specifically call out restrictions on key devices:

- prohibit the use of portable data storage media and devices except with specific permission,
- prohibit the use of a computer's USB ports without specific permission,
- prohibit the connection of MP3 and video recorders and players to PCs,
- restrict connection of personal PDAs to company-owned PCs,
- prohibit the connection of personal mobile phones and cameras to PCs,
- limit the capacity of data storage devices issued by the organization, and
- limit data copying to key staff or departments.

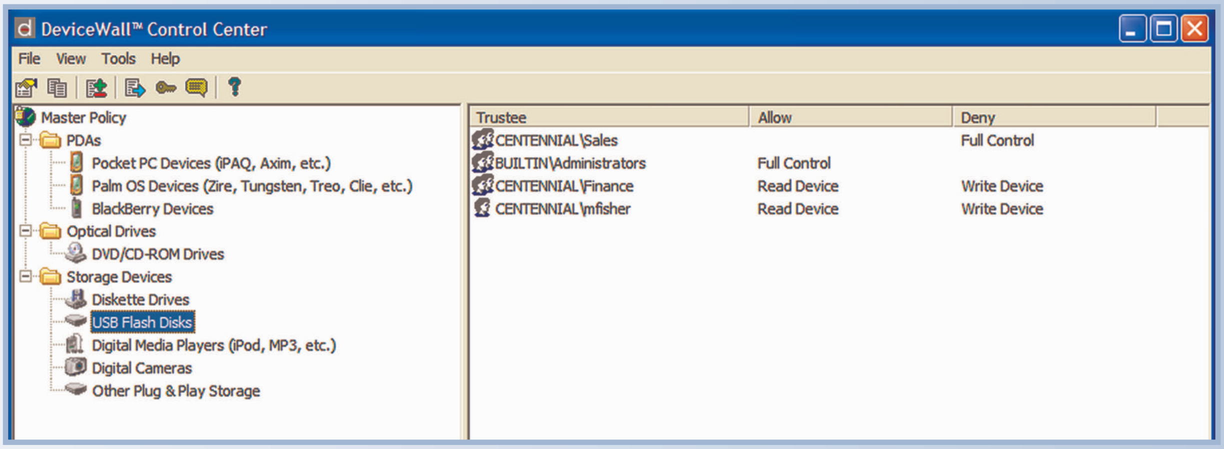
In addition to updating their lifestyle device policies, organizations should also develop a simple matrix (see, for example, Table 1) that clearly spells out who is authorized to use or connect certain equipment types.

The AUP should also clearly spell out why these devises pose such a serious threat:

- *Loss of confidential information*. The unauthorized release of confidential information can present huge problems for businesses, ranging from a loss of competitive advantage to a loss of reputation or brand damage, or even to court action. Industrial espionage occurs most frequently when employees change jobs and carry digital assets—customer databases, supplier lists, financial information, and product plans—from their current to their new employer.
- *Intellectual property rights infringement*. Most of the content accessed by employees, whether it is held locally or on the Internet, is subject to some form of intellectual property or copyright law. This is reason enough for organizations to keep sensitive information inside their networks, but they should also be concerned that the unauthorized transfer of this property can open them to possible prosecution by the copyright owner.
- *Corruption of data and systems*. Although an overwhelming majority of organizations have antivirus solutions in place, 68 percent of businesses suffered at least one virus infection in 2004, with two-thirds of these reporting a virus outbreak as the year's "worst incident" (*Information Security Breaches Survey 2004*, Price Waterhouse Coopers and United Kingdom Department of Trade and Industry, Apr. 2004). Although most organizations have taken steps to protect themselves from the primary avenues of virus propagation—e-mail and Internet downloads—many are still susceptible to malicious code being introduced directly through a PC on the network.
- *Vicarious liability*. Put simply, vicarious liability means that an employer can be held responsible for its employees' negligent acts, regardless of whether the employer authorized them. In addition to data loss or threat introduction, employers face significant risk if employees use their networks to transfer inappropriate content.
- *Breach of privacy and data-protection laws* (such as Sarbanes-Oxley and the Gramm-Leach-Bliley Act). The list of regulations governing compliance for content and data seems to grow every day. With increasingly strict data-protection laws in place, organizations lacking con-

Figure 1. Centennial Software's Device Wall is one of several new security utilities that monitors and protects ports on PCs in local and distributed networks.

In the primary management screen (displayed here), devices are divided into categories based on device type, and each category is associated with users or user groups.



- Master Policy
  - PDAs
    - Pocket PC Devices (iPAQ, Axim, etc.)
    - Palm OS Devices (Zire, Tungsten, Treo, Clie, etc.)
    - BlackBerry Devices
  - Optical Drives
    - DVD/CD-ROM Drives
  - Storage Devices
    - Diskette Drives
    - USB Flash Disks
    - Digital Media Players (iPod, MP3, etc.)
    - Digital Cameras
    - Other Plug & Play Storage

Trustee	Allow	Deny
CENTENNIAL\Sales		Full Control
BUILTIN\Administrators	Full Control	
CENTENNIAL\Finance	Read Device	Write Device
CENTENNIAL\mfisher	Read Device	Write Device

trol over information leaving and entering the network can face investigation by industry watchdogs such as the US Securities and Exchange Commission, or even prosecution for company principals.

Having defined an AUP, the organization must distribute it and require its employees to acknowledge it. Again, it's not that these threats didn't exist previously, or that they weren't included in previous AUPs. But because the ease of "grabbing" this data increases exponentially with each newer and more capable media player or memory stick, organizations should elevate both the seriousness of these threats and their planned response to them.

GOVERNING AND ENFORCING THE AUP

With the USB and FireWire connections on networked PCs serving as the critical link for lifestyle devices, a tool that can remotely manage access to these ports appears to be the key to mitigating the risks outlined in the AUP (see, for example, Figure 1). Although the ports are fundamentally hardware connections, they are strictly controlled by operating system software. For this reason, as well as practical matters such as cost, scalability, and overall management, the best solution for managing an AUP's enforcement and monitoring will likely be a software solution. Any such client-server-based network-wide solution will need to

- manage device access among multiple users and user types;
- set rules for permissible devices, blocking all other uses;
- provide temporary access when necessary; and
- gracefully educate users on the new system's rules and expectations.

As Table 1 outlined, organizations should base acceptable use on both the device in use and the type of user attempting to connect it. The optimal solution should be able to adapt to pre-existing user-management structures, such as Microsoft's Active Directory (AD) or Novell's eDirectory, but not depend on them for its deployment or routine management. Permission to access and use external devices should be grantable at both the group level, using Lightweight Directory Access Protocols (LDAPs), such as AD or eDirectory, and Microsoft Management Consoles (MMCs), and the individual user level. Considering the impact of deploying any new client-side tool in modern networks, the best solution would be self-deploying, or would integrate with some other deployment tool (see the "Products for Further Research" sidebar).

The device types reflected in the AUP—such as PDAs (Pocket PCs, Palms, and Blackberries), optical drives (CD and DVD drives), and storage devices (iPods, memory sticks, compact flash cards, and cameras and camera cards)—should manage the user-to-device associations.

The solution should also control and manage usage levels. For PDAs, this might mean granting synch, read, and write permissions only to highly mobile employees, such as sales and tech reps (see Figure 2). For optical drives, you might grant "read only" permissions for most employees, but "write" permissions for marketing and product support teams. Devices should be identifiable by class, so IT managers can block access to iPods and other audio and video recorders, while allowing access to memory sticks if the user group needs them. The administrator should be allowed to fully block any storage device class or allow read-only access to it.

Perhaps future versions of these solutions will include settings that prohibit transferring certain files or file types to external devices, or that automatically encrypt files transferred to inappropriate locations. To add traceability (perhaps the strongest deterrent to casual misappropriation of sensitive documents), logs could record the movement of files from network servers to external devices. A major counterthreat to the accessibility of lifestyle devices could be a central data store that "knows" what files are copied to which devices on which employees' computers, and when and where the copying occurred.

A fundamental conflict of network security is the need to provide the highest level of protection without adversely impacting network or end-user productivity. The same tension will exist in the management of lifestyle computing devices. The optimum solution should be able to easily override security settings from the central console, temporarily granting device access to users with specific needs. Administrators should be able to manage this from the network console, but some vendors are already supplying functionality that lets remote PC users who are not on the network request temporary access. Centennial Software's Device Wall, for example, includes an elegant, key-coded override utility that can grant temporary access to specific device types. The field user simply calls their home office's IT help desk, exchanges codes, and specifies what device type they'd like to use. With the code exchange, the device is accessible and ready for use.

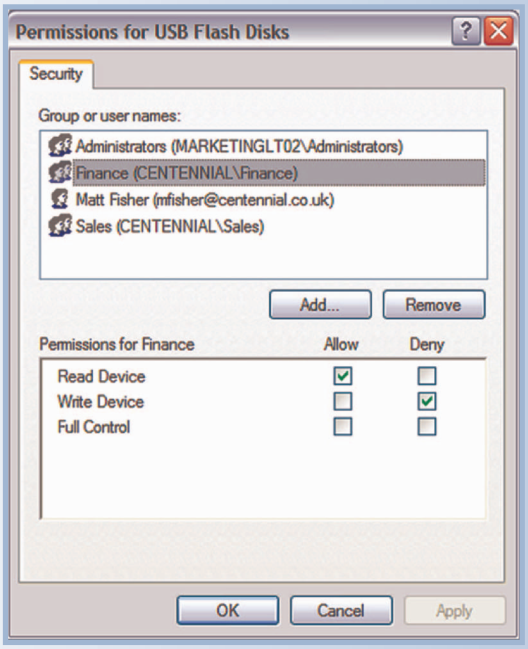
With the introduction of a network-wide system for managing storage devices and peripherals, users will have to adjust their plug-and-play expectations. The products that best solve the problems outlined here will give feedback to end users who try to plug in iPods and memory sticks, gracefully telling them that the requested device is not accessible. It could refer the user to the organization's AUP or list the attached but

Products of Further Interest

- **Device Wall by Centennial Software:** http://www.centennial-software.com/dev/index.html. Device Wall comes close to fulfilling all of the requirements outlined in this article. Developed by network auditing and deployment experts, Device Wall secures USB and FireWire ports, and optical and magnetic drive access. It manages permissions based on user groups and types, works with Active Directory or can create its own scheme, and can piggyback on Centennial's Discovery software for rapid deployment. Centennial's experts contributed to the acceptable use policy outlined in this article.
- **Sanctuary Device Control by SecureWave:** http://www.securewave.com/sanctuary_DC.jsp. Luxembourg-based SecureWave's Sanctuary Device Control secures ports and allows for a "white list" of acceptable devices. Scheduled device access can provide additional flexibility while still maintaining security. Sanctuary addresses most of the requirements outlined in the article.
- **DeviceLock by Smartline:** http://www.protect-me.com/dl/. DeviceLock has many of the other products' features, but requires Active Directory for support and permission assignment. It works with Windows 2000 and Windows XP clients.

Figure 2. In Device Wall, individual screens control rules and permissions for devices within a given category.

Permissions range from partial control of the device, such as read-only or write-only control, to full control or an "access prohibited" state.



Permissions for USB Flash Disks

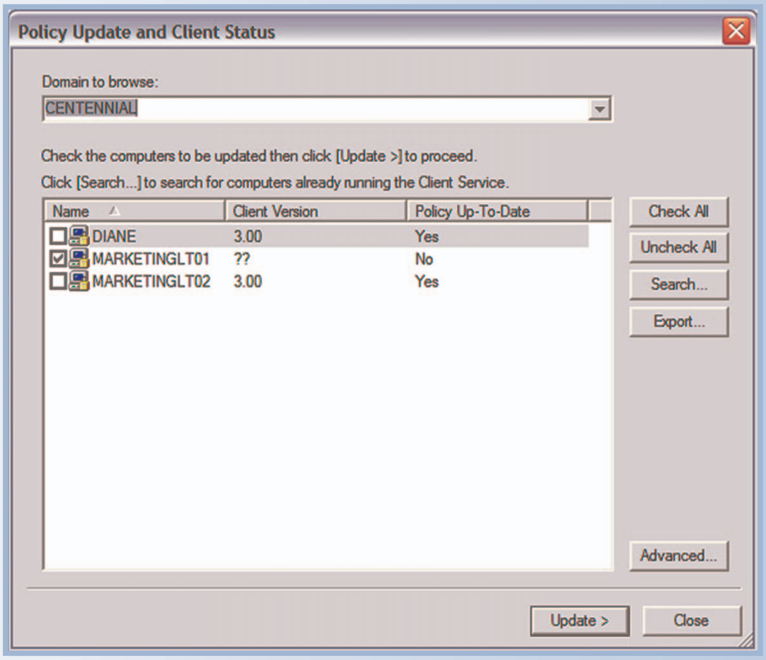
Security

Group or user names:

Administrators (MARKETINGLT02\Administrators)
Finance (CENTENNIAL\Finance)
Matt Fisher (mfisher@centennial.co.uk)
Sales (CENTENNIAL\Sales)

Permissions for Finance	Allow	Deny
Read Device	☑	□
Write Device	□	☑
Full Control	□	□

Figure 3. A dialogue screen provides information on the status of each group or individual policy, provides options to immediately update policies or export them for use in other implementations, or find PC clients that are running the software.



Policy Update and Client Status

Domain to browse:

CENTENNIAL

Check the computers to be updated then click [Update >] to proceed.

Click [Search...] to search for computers already running the Client Service.

Name	Client Version	Policy Up-To-Date
☐ DIANE	3.00	Yes
☑ MARKETINGLT01	??	No
☐ MARKETINGLT02	3.00	Yes

blocked devices. For greater flexibility, implementation in open environments such as university computer labs or libraries could use a quiet mode that simply blocks connections without informing the PC user.

Of course this communication layer's back end should include reporting to the IT staff managing the solution. Reports could specify how many clients the solution is in force on and how many devices it has denied, show policy changes and their effective dates, and detail any exceptions (see Figure 3 for an example).

LESSONS FROM THE MARRIAGE OF ANCIENT HISTORY AND CURRENT TRENDS

The impact of illegal or improper activity will increase exponentially as super-sized hard drives branch into every device and every aspect of life. A recent *Scientific American* article quotes Seagate CTO Mark Kryder's succinct view of this proliferation: "In a few years the average US consumer will own 10 to 20 disks drives in devices he uses regularly" (Chip Walter, "Kryder's Law," *Scientific American*, Aug. 2005). Not only will the drives be pervasive, but, according to the article, their capacity will increase at a rate that outstrips Moore's Law, which in the early 1980s accurately forecast the doubling of processor capabilities every 18 months. Storage devices are currently experiencing 40-fold increases every four years, and Kryder's goal is a terabit of storage within a square inch—enough to record 2,000 full-length digitized movies, or the contents of an entire corporate file server.

Access to optical and disk drives, media devices, cameras, and memory sticks might not be today's biggest threat to network security, but as these devices become more powerful and available, it is irresponsible to ignore the threats they represent for much longer. If the IT manager's biggest fear is someone inserting a lethal virus or worm into a network, the CEO's biggest fear is a disgruntled sales representative copying the company's prospect database into his or her personal iPod.

The Great Wall Syndrome might be characterized as a belief that the only security that really matters is the one around the organization's perimeter. With decentralization becoming an increasingly common trend in networks, it is more appropriate to think in terms of many small walls rather than one huge one. Each small wall would surround a vulnerable node at the client, preventing its connection to increasingly fast, potent, and portable devices. With each of these small walls communicating to a central server to obtain policies and report on the system's efficacy, the resulting security might prove to be as important as the perimeter defenses.

A metaphor comparing holes in client PC security to the fatal breach in the Great Wall of China might seem a bit of a stretch, but technology tips the scales toward defender and invader alike. Legend says that when Wu Sangui opened the door at the Shanhai Pass, it took three full days for the massive Manchu army to pass through the yawning gate. Today, an iPod can hold around three quarters of a million average Microsoft Word documents, and it can capture them in minutes. It's difficult to say which scenario is more frightening. ■

Michael Thelander *is director of product management for Portland, Oregon-based Chrome Systems, and a freelance science and technology writer. Contact him at michael@thelander.net.*