fours under your desk to unplug one device so you can plug in another. Going wireless will also allow effortless networking of electronic devices. Gone will be the clumsy workarounds you have to employ when you want to use a stationary, networked printer to print from your laptop or deliver a PowerPoint presentation using unfamiliar A/V equipment. You will be able to simultaneously transfer digital images from your still or video camera straight to a printer or external hard drive, play music directly from your iPod to your stereo speakers, and send a scanned image to your computer—all without any physical connections.

Initially, wireless USB hookups will happen via a dongle—a small device that plugs into a computer to authenticate software, expand memory, or facilitate communication—connected to the host's USB port. The dongle will exchange signals with a USB hub or a transceiver plugged into a peripheral. Soon after, computer and device makers will start embedding wireless USB interfaces in their products, making the dongle-and-transceiver setup unnecessary except with legacy computer systems and devices.

That's the good news. But for every silver lining there's a cloud. The confidence that comes from knowing exactly what you're getting when you see the letters USB may not hold for its wireless incarnation—at least not in the early going. Here's why:

Wireless USB will transfer data over a short-range, low-power, high-data-rate communications technology known as ultrawideband (UWB). In this approach, the transmit power of the digital signal is spread across a broad swath of the spectrum, emitting just a tiny amount in each frequency. Although UWB uses portions of the spectrum "owned" by other users, interference is limited by the fact that its low power output makes its transmission on any given frequency indistinguishable from noise.

Two camps—one led by Freescale Semiconductor Inc., based in Austin, Texas and an offshoot of Motorola Inc., and the other by Intel Corp., in Santa Clara, Calif.—are vying for the right to call their versions of UWB the worldwide standard. The fight over which group's technology would be named the IEEE 802.15.3a UWB standard dragged on for more than two and a half years [see "Ultrawide Gap on Ultrawideband," *IEEE Spectrum*, January 2004]. Then, in January 2006, the IEEE standards group finally acknowledged that the stalemate would not be broken, and it voted to disband. Now both UWB technologies—and the technologies that they enable, such as wireless USB—will have to fight it out in the marketplace. Until consumers declare a winner, there will be two incompatible types of wireless USB.

Freescale was the first to produce chips that made wireless USB over UWB possible. At the 2006 International Consumer Electronics Show in Las Vegas in January, Belkin and Gefen demonstrated prototypes of the aforementioned wireless USB devices. Belkin's four-port hub communicates with a dongle containing a UWB radio made by Freescale. USB devices plug into the hubs with cords, but the

## CYBERCRIME AT A GLANCE

Whether it is an experiment by an amateur virus writer somewhere in India, done just for the individual's personal entertainment, or the carefully planned and executed for-profit scheme of an Israeli spyware company, a computer security attack is annoying and damaging.

But just how much damage can cybercrime cause? About US $67 billion to U.S. companies last year, according to an estimate based on the Federal Bureau of Investigation's 2005 *Computer Crime Survey*, released in January. The FBI questioned 2000 public and private organizations in four states and extrapolated some of the results to the rest of the country. It found that viruses and spyware were the most common problems reported [see table], while the effects of viruses and worms were the most costly. The attacks came from 36 different countries, with half of all the attacks originating in the United States or China.

A small fraction of the organizations reported the incidents to law enforcement officials. Most of the others were either unaware that the attacks were illegal or believed that law enforcement would not help them—and might even harm them.

"There's this incorrect myth that once you call law enforcement, you're going to have your hard drive and files taken away and you'll lose your business because all your equipment is gone," says Tim Rosenberg, a research professor at George Washington University, in Washington, D.C., and CEO of Lancaster, Pa.–based White Wolf Security. Many companies also wrongly believe that reporting the crimes invites negative publicity.

What can organizations do about the pervasive cybersecurity threats? According to Rosenberg, companies need to stop measuring security investments just in monetary terms. He says that companies should start thinking of information security as a kind of marathon. "It's a lifestyle," he says. "It should affect every decision you make every day. You can't eat healthy and then not work out...you must change your lifestyle."

—PRACHI PATEL-PREDD

**US $67 billion**
Estimated financial losses from security attacks in the United States, extrapolated from survey data

**$32 million**
Financial losses from security attacks reported by respondents to the FBI

**$12 million**
Respondents' losses from viruses and worms

**90%**
Portion of organizations sampled by the FBI that suffered a cybersecurity attack

**84%**
Portion of respondents that had virus problems

**9%**
Portion of those organizations that reported the problem to authorities

**79%**
Portion of respondents that had spyware attacks