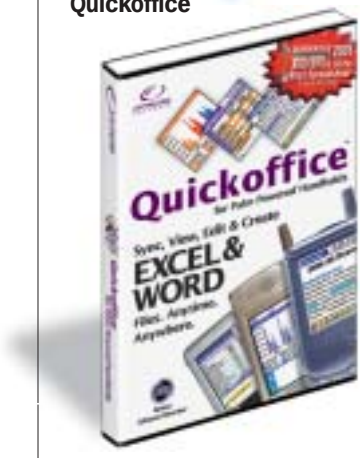
tools of the trade

Quickoffice



Find It, Fix It, and Add Some Functions

Quickoffice from Cutting Edge Software, Inc. is an award-winning suite for Palm PDAs that lets you create and edit, sync, and view Excel and Word documents on your PDA. It has four components: the Desktop, Quicksheet, Quickword, and Quickchart. Desktop runs on your PC, facilitating the synchronization of your Word and Excel documents from desktop to handheld. Quicksheet is a spreadsheet for your PDA with more than 60 built-in financial, scientific, statistical, date and time, table, and aggregate functions. Sorting is by row, column, or selected region. Quickword imports Microsoft Word documents that you can then read and edit. It has auto-scrolling for continuous reading, left and right justification, choice of four font sizes, word count statistics, find and replace functions, and other familiar doc capabilities. Quickchart provides the five most popular charting views from within Quicksheet.
www.quickoffice.com

AscToHTM from Jafsoft is a tool that performs the relatively esoteric task of converting plain text to a format (HTML) that can be loaded on a website. If your website is underutilized because it's too much of a hassle or too expensive to redesign documents so they can load properly online, this very inexpensive tool could help you fill some of the empty space. Company newsletters, policy documents, announcements from HR, white papers, and even tables can be converted in a simple two-step procedure for non-coders. You select the file and its output name, and then hit the convert button. AscToHTM converts ASCII text, so if the original is a Word or WordPerfect document, you have to open it and resave it as plain text, but you won't be typing HTML tags. AscToHTM recognizes headings, bulleted lists, emphasis, tables, code samples, and ASCII art in the originals, and it can handle several languages. You can even fine-tune policies you want applied to documents to be put online. There is a demo you can download at www.jafsoft.com.

Popups aren't only annoying, they also use up memory when they remain open under the current page you are viewing. With a name that belies its technical efficiency, STOPzilla is one of the best utilities for managing and eliminating the popups, spyware, and unwanted cookies that are sometimes placed on your computer without your even noticing. The program is extremely simple

AscToHTM converter

Securing the Hardware

Michael Castelluccio, Editor

A STOLEN LAPTOP might turn out to be no more than an expensive annoyance, or it might create a credible threat to national security. A lot depends on what's on it. Sometimes even the loss of computer parts, say, hard-drives from a research laboratory, can create significant panic. So what can a company or agency do to secure its computing hardware?

It's certainly not getting any easier. The targets are getting smaller and lighter. Even PDAs, with their increased computing and network capacities, can be a significant loss depending on what they are loaded with and what they're connected to. And hardware can even be heisted "virtually" without any need for screwdrivers or bags. A back-door entry over a network can empty a hard drive just as efficiently as if it were pried out of the desktop or server. More so maybe, because without the broken glass or opened locks, you might not even notice the loss for a while.

One way to approach the problem of hardware security is to examine the methods that are currently working for the bad guys and fix those first. For this, the Brigadoon Software *1st Annual Computer Theft Survey* is a good place

continued on next page

STOPzilla Popup Blocker

with an alert, a single-button choice, and an automatically updated blacklist of popups and wares you don't want to load on your browser. Offered as an annual subscription, like virus-blocking software, there's a free download that lets you try the program first. www.stopzilla.com

Own a PDA long enough, and one day you'll drop it, bump it, or sit on it and crack the screen. I've seen the dread pattern of irregular lines in two of my own devices. The first time, I sent the device out to be repaired, but the second time I saved more than half the cost by getting a replacement screen from GetHighTech, Inc. at PDA Parts.com. If the screen is broken and you replace it with a complete screen/digitizer, the repair involves loosening a few screws, unplugging the screen's ribbon plug, and slipping in the new screen/digitizer. If you are only going to replace the glass, there's the added step of separating the digitizer circuit from the original glass. Go to www.pdaparts.com to see what the screens look like and to see a demo of how they are replaced. It's also a good place to look for other replacement parts, accessories, refurbished PDAs, and even a repair service.

GetHighTech Replacement Screens

PC PhoneHome Recovering Stolen Computers

Brigadoon Software, Inc. has an interesting solution for stolen computers. It's a tracking and theft-recovery software that keeps tabs on where your computer is by sending a stealth e-mail every time you boot your computer. You determine where the e-mail is sent, so you control the tracking (no yearly monitoring fees). Brigadoon's Software Command has recovery agents who work with you and law enforcement to locate and recover the stolen computer(s). There are four versions of the software: PC PhoneHome™ for desktops and laptops, for Pocket PCs, and for the enterprise and MacPhoneHome™ for Macintosh computers. See Tech Forum for a description of Brigadoon's Annual Computer Theft Survey. www.brigadoonsoftware.com

continued from p. 55

to start. Brigadoon is a New York software developer that has a LoJack-type of solution to protect PCs, PDAs, and Macintosh computers. (See Tools of the Trade, page 55.)

Terrance L. Kawles, president of Brigadoon Software, says the survey "fills a void in the collective body of knowledge of computer security." It's the first survey dealing with the specific issues of the theft of computing devices. Kawles explains, "It was designed to be international in scope and covers all issues surrounding the theft of computing devices in great detail." (The 27-page report is available at www.brigadoonsoftware.com.)

The survey is based on the responses of 676 participants in the following general categories: individuals, corporations, students, academics, and military/government. About half were from North America, 25.1% from Europe, and the remainder from the Pacific Rim, Africa, South America, Asia, Central America, and the Middle East.

The Numbers

In response to the question "How many times has your organization been the victim of computing device(s) theft in the last 12 months?" almost half (44.5%) said they had been victimized. Of the devices stolen, laptops were the most popular (48%), then desktops (26.7%). PDAs (13.3%), Tablet PCs (4%), and Internet-related mobile phones (2.7%) rounded out the list. Unfortunately, 99% of the respondents victimized said the thief was never caught—a very disturbing number when you also consider the fact that 88% of the respondents didn't encrypt the proprietary data on their stolen devices.

The answer to the question "When did the theft occur?" offers some insights into what should be in companies' security policies. The significant "During business hours" response (29.9%) breaks down into from cubicle (9.9%), from open bay area (12.3%), and from private office (17.2%). In these areas, cables and other locks might prove effective. But because 53% of thefts occurred "while respondent[s] were mobile (moving about)," other measures are required to protect information (passwords, encryption) and the devices themselves (tracking devices or software).

Unfortunately, 99% of the respondents victimized said the thief was never caught—a very disturbing number when you also consider the fact that 88% of the respondents didn't encrypt the proprietary data on their stolen devices.

Other considerations for those creating a security policy are the fact that 92.7% of respondents use only a log-in password to protect their computer, and 68% said they "only back-up data weekly, monthly, rarely, or never." For some, the disappearance of a computer means the permanent disappearance of the information on it. For others, the loss of proprietary information is even more costly than the device stolen. In either case, it's possible to save and secure the information on a machine that leaves the office.

The numbers describing security policies aren't reassuring. A surprising 89.6% of respondent organizations "do not have written guidelines on protecting proprietary information on computing devices while traveling," and "76.2% do not have written guidelines on how to respond to the theft of a computer."

In estimating the total cost of computer theft, the final numbers included the cost of replacing the hardware, the cost of the information, the loss of productivity, and the downtime caused by the theft from a low of one day (19.4%) to more than one month (6.0%). The final number was $14,227.27 per computing device stolen. The cost in dollars for proprietary information on the device can be much higher.

So Where Do You Start?

There is much more information in the survey than we have looked at here, and it's a great place to begin if you are considering a security policy for your company or just a mental checklist of your own to help you hang on to your computers and information. Physical barriers can be effective in some areas, while software/hardware solutions might work better for some. Look at Brigadoon's tracking software. Check out the fingerprint verification systems or the chips you wear on a lanyard that let only you boot the machine. Learn how to encrypt the more sensitive information on your machine, or develop really strong passwords. And back up everything. With CD burners on most new machines, it's very simple to save and store elsewhere what you need. If it's a PDA you're using more often now, do a Google search on Back-up Buddy or other similar programs that make back-ups on those devices easy. And synchronize with your desktop every day. ■