Computer News for Law Firms

No. 28 | Heckman Consulting llc | Fall 2004

How Secure is "Secure"?

With the release of Service Pack 2 for Windows XP, the topic of computer security has been much in the news lately. What does "computer security" really amount to? How secure is "secure?" Most importantly, what is realistic for a small to medium-size firm? The first thing to understand is that with the constant release of new technologies (and new techniques for hackers to break them), "security" is both relative and a moving target. The first step in evaluating security issues is to start with certain basic conceptions.

The bottom line about security is that the more secure you want to make a system, the harder and more inconvenient it will be to use (and the more money it will cost). This is true in virtually all areas, from turning on a PC to flying on an airplane. In addition, "increased" security can be self-defeating: witness a firm that decided to enforce difficult-to-guess passwords (both numbers and letters and nothing that would be a "word"). Virtually all users attached their passwords to their monitors with a yellow stickie, so the net result was less security, not more. Similarly, increased airport "security" has resulted in an increase in baggage theft.

When making decisions about security, a firm must decide what its comfort level is. If your "comfort level" means no security, at least that decision should be made consciously with some awareness of the risks involved.

Heckman Consulting

Heckman Consulting is a systems integration firm specializing in the legal market. John Heckman has over 20 years experience in the legal community. For back issues of this newsletter, go to www.heckmanco.com. After seven years in Connecticut, we recently relocated to the New York metropolitan area. You can now contact us at:

Heckman Consulting
372 Fifth Street
Jersey City, NJ 07302
Tel: (201) 792-0022
Fax: (201) 792-9542
e-mail: heckman@heckmanco.com

What Are the Risks?

When approaching the question of security, people's reactions range from "What Me Worry?" to a computer version of agoraphobia: refusal to use the Internet because it is too "risky" (so is crossing the street). Without a realistic assessment of the risks involved it is impossible to work out a strategy for minimizing them that you are comfortable with. This is complicated by the fact that an event with a very small risk could have catastrophic results (total loss of data).

Fundamentally, there are two types of risks: random and targeted. You could be run over by a car just crossing the street or because somebody is trying to kill you. Random risks are by far more common and tend to fall into the following categories:

Spam. This can be more than just an annoyance. Many spammers take over your PC and use it to re-broadcast spam messages, which can cause your Internet Provider (ISP) to claim you are a spammer and discontinue your service. Some clients have spent up to two weeks getting their e-mail accounts re-enabled when this happened.

Spy-Ware. Many "free" Internet programs install secret "spy-ware" programs to monitor your PC and send your preferences back to the maker of the program to use for further marketing. In addition to invading your privacy (they claim that by clicking OK to install the "free" program, you agreed to this process), these programs can seriously slow down your PC, cause crashes, and generally interfere with its functioning. Both Dell and Microsoft have recently estimated that over half the tech support calls they receive concerning computer crashes can be traced to spy-ware related issues. There are a number of anti-spy-ware programs that identify and eliminate such programs. One of the better ones is Pest Patrol (www. pestpatrol.com - which also has a corporate version for networks). A sub-set of these programs generate the ubiquitous pop-up ads. Programs such as Ad-aware or browsers such as Mozilla/Firefox can help eliminate these pop-ups. If you want to use a program that has both "free" and paid versions, it is almost always worth getting the paid version to avoid spyware/adware problems. With any of these programs, you will have to take some time to configure it initially.

Phishing. This used to be known as "social engineering." You receive an email purporting to come from a major bank, credit card company, on-line auction house or even Microsoft. It "warns" you that your account is about to be cancelled unless you go to a web site "re-register." The web site "looks" like a real one, but actually steals your credit card, bank information, etc. Wells Fargo and Citibank have recently been victims of these attacks. Banks, credit card companies and Microsoft *never* use email for this sort of notification. These emails are *always* fraudulent and should be deleted without opening them.

Worms and Viruses. You have heard it a thousand times, but you should always run an up-to-date anti-virus program. "Trial" versions that come with new PCs are *not* up to date. The yearly subscription for anti-virus programs should be considered "insurance," akin to your car or house insurance. In addition to potential damage to your PC, variants of these programs can turn it into a "zombie" used in attacks on various web sites or other institutions. A recent article noted that one ISP had identified a system that was using 10,000 remote "zombies" to attack web sites. You could have been among the 10,000 without even being aware of it!

War Driving. If you have a wireless network, you are susceptible to "war driving" - people who drive around with a laptop in their car seeing what wireless networks are available and how to invade them. If you insist on a wireless network (a bad idea), you should hire a knowledgeable consultant to secure it. The most basic step is always to change all the default settings immediately. Wireless networks are by nature quite insecure (in addition to being very slow for anything but checking your email).

(Continued over)

How Secure? *(Cont.)*

Targeted Attacks

What if somebody is just "after you"? This is akin to industrial sabotage and is relatively rare for smaller firms, unless they are involved in high-profile cases or cases that become highly emotional such as divorces. However, by far the most common case of this sort comes from disgruntled employees who are planning to leave and want to do some damage. This last category is much harder to protect against without expressing a vote of no confidence in your staff (which then has repercussions for morale).

What Can You Do?

There are two ways in which you can improve your security: adding specific programs aimed at making your system more secure and configuring your existing programs. You should have four types of utility programs: anti-virus, a firewall, anti-spam and anti-spyware/adware programs. Even more importantly, these must be kept up to date virtually on a daily basis (fortunately, most of these programs can be set to auto-update). If you do all this, your cost is likely to run around $100-200 per PC. For a useful (if partial) source of information, see www.spywareinfo.com/downloads.php

Adding Utilities

The four main anti-virus programs are made by Norton, McAfee, Trend Micro and Panda. Norton and McAfee also sell packages that include other features in addition to anti-virus, but these are generally not as robust as standalone products.

If your firm has a network firewall, you may not need a separate one. Some features are built into Internet routers, but you should consider running a program such as ZoneAlarm, which blocks outgoing as well as incoming items, thus preventing spammers from hi-jacking your computer. The "firewall" included in Windows XP 2 does not do this.

There is a wide range of anti-spam software and email products (such as Outlook or the email client included in TimeMatters) are starting to include rudimentary anti-spam features. A good anti-spam program includes three types of protection: "white lists" (let all email from this address in); "black lists" (don't let any email from this source in) and baysian filters that train your program what to accept and reject based on content analysis and your response to incoming mail over time. Mailwasher is a favorite for many people.

Anti-spyware/adware software prevents these programs from sending marketing information about your preferences back to their makers for re-sale, analysis, etc. In addition, they also include "popup blockers" that can stop all those annoying messages. PestPatrol, SpyCop and Ad-aware are three of the best (again, you would be well advised to get the paid versions).

Configuring Your System

I have dealt with configuring your PC at greater length in previous newsletters (see Newsletters nos. 22 and 24 on my website, www.heckmanco.com). One simple thing to do is to stop using Internet Explorer and start using Mozilla/Firefox or Opera. The consensus of computer publications at this point is that these are both better browsers than IE, and are definitely much more secure. In fact, for the first time in years, IE has begun to lose market share to these browsers. There may be some sites that insist on ActiveX controls that you still need IE for, but you can greatly reduce your risk by switching.

In addition, you should turn off the preview pane in Outlook to prevent viruses from executing automatically (since a message is "opened" as soon as it appears in the preview pane). In Outlook XP, click on View | Preview Pane. In Outlook 2003 under "View" you must turn off *both* the Auto Preview and the Reading Pane

Lastly, you should eventually install Service Pack 2 for Windows XP (Microsoft does not plan to implement additional security for previous versions). I say "eventually" because at present reports indicate that about 10% of all PCs have problems with SP 2. In addition, before installing SP 2 (get the CD: the download is huge), you should check with the vendors of all your legal-specific or other specialized software to make sure they are compatible or that a patch exists that can make them compatible. When SP 2 first came out, Microsoft released a list of about 60 software programs (including some Microsoft programs) that were incompatible with SR2. Over time, programs are fixing their compatibility, but you may well have to spend a couple of hours tweaking your system in obscure ways after installing SR2. ■

Heckman Consulting llc
372 Fifth Street
Jersey City, NJ 07302

Stamp

Tel: (201) 792-0022 Fax: (201) 792-9542 e-mail: heckman@heckmanco.com Web: www.heckmanco.com