AccountingSoftware 411 .com the Insider
In-depth research, analysis and insight for the accounting software industry
www.AS411.com

How Secure is Your Computer Security - Part 1

By Richard Oppenheim CPA CITP

This article appears in two parts:
1. Getting ready for improving computer security
2. Planning and implementing computer security

There are uncountable articles that discuss security surrounding the use of computers. This information includes protection for applications, correspondence, internet access and yes, even games. The news of the day is often filled with reports of computers being stolen, discarded, corrupted and set on fire.

Some of the recent headlines include:

- Ten computers stolen from Nashville-based hospital firm
- Missing data involves thousands of files on unpaid Medicare, Medicaid bills
- Computers Stolen in Ohio with 72,000 Medicaid Subscribers' Personal Info
- 5 Computers Stolen From Capistrano School District
- Laptop Computers Stolen from School in Washoe County
- Truck containing computers stolen from Botetourt Co. truck stop
- 31 notebook computers stolen from SME Bank

Computer security is not a new issue. It has been around since the integration of mainframes, minicomputers and personal computing within our business environment. Consequently, the need for security should NOT be a surprise. As the headlines above indicate, the potential loss can be just equipment or just the data or both. Losing encompasses the replacement cost as well as the potential loss of confidential information.

We live in a risk filled world. Within the world, computing has evolved to an omnipresence that has technology showing up everywhere for every one 24 hours per day. With the every moment use, everything from weather disruptions to natural disasters to equipment failures to bad people makes the management of our business and personal lives complex. Establishing security around your computer equipment and resources has to start at the beginning – know what you have. All of the issues surrounding security have to be targeted at protecting the assets, resources and business functions within the enterprise.

Your computer security starts with knowing the total range of information about your firm. One part of that information range is the computing technology and supporting assets. The firm needs to maintain an inventory of computers and the applications along with the data that have been installed on each computer. Examples of data include content from typical applications such as tax, audit, consulting, financial planning, record keeping and so on.

Firm management needs to be proactive about computer security. There is a requirement for research and analysis and a call to action for an on-going and evolutionary set of procedures.

For the research and analysis, it is important to know that there is no such a thing as absolute security.

- Computers fail
- Computers get lost
- Software is not perfect
- Data gets lost, copied, misfiled
- Privacy gets compromised
- Any computer connection is a risk

In this article, we will focus on computer security through 4 basic categories:

- Resources
- Environment
- Attacks
- Planning

Resources

Resources encompass everything that is available to support the firm operations. This includes personnel, physical office space, furniture, fixtures, paper, and all technology products, data and services. Basic firm information should be accessible by every partner and manager. This includes: street address and building access information, owner/landlord contact information, other CPA firm partner and associate offices information, telephone and voice communications products and services, internet access, and backup facilities location and access information.

Keeping focus on technology, all documentation about computer and information assets needs to be current. To accomplish this, data collection has to start at the time of acquisition, including: information about the computer features, programs installed, data type (word processing, spreadsheets, tax data, etc) and connectivity functions (networking, wired vs. wireless, etc).

Clearly all collected information has to be current. Having last year's password provides no benefit. Other firm information that needs to be documented and retained offsite are:

- Legal Data
- Contracts
- Patents, Trademarks, etc
- Employee Agreements
- Policy and Other Manuals

Another major resource within the firm is the people. Different groups of people include:

- Staff
- Managers
- Techies
- Shareholders
- Contractors
- Customers
- Visitors
- Regulators
- Suppliers
- Professionals

Keeping data about each group facilitates the ability to contact them for alerts about problems such as theft or unauthorized release of confidential information. Moreover, if the office is shut down and access is not immediately available, you will have the means to contact people who may be trying to contact you.

Environment

Books can be written about the environment and the issues that need to analyzed. While the selection of location has several business considerations, the potential risks of any location include:

- Possible weather issues (hurricanes, tornadoes, earthquakes, snow storms)
- Possible flooding through proximity to oceans, lakes or rivers
- Proximity to nuclear plants
- Age of the building and its construction stability

Under the environment category are all of the physical access concerns, such as door locks, window locks, and other defenses necessary to protect the inside from intrusion by unauthorized bad guys. In this regard, it may be helpful to know your neighbors and the potential risks that staff or frequent visitors may create. For example if your office is right next to a coffee bar, the traffic of people walking past your front door may entice someone to make an unauthorized entry.

When analyzing your office needs you MUST include everyone's home office. Typically, a lot of computer equipment and confidential data are located in the home, or transported in a vehicle. Protections and security for these areas has to be carefully considered.

Attacks

Computer attacks can occur as a result of:

- Intentional act by one or more persons
- Accidental events where people make mistakes such as deleting current data
- Nature events such as weather, floods
- Old Age which is a cause of computer or building failure

You have to decide how to protect against each of these attacks. Protecting the premises from the dangers of a flood, for example, is a far greater concern in New Orleans than it is in Denver. However, Denver residents have to consider snow storms and New Orleans does not.

The potential for dangerous events has to be part of your analysis. In fact, it may be useful to retain outside experts to assist with this process.

There can be attacks against your computers every day, if not every hour. Typically attacks are done through some form of malicious code. The names given this variety of code attacks are:

- Trojan Horse
- Worms
- Virus
- Spam
- Spyware
- Phishing
- Scam
- Hoax
- Denial of Service

The firm's strategy has to focus on the installation and maintenance of defenses against any of this potentially damaging code. The code arrives most often through an attachment to an email. It can also arrive as a download from any web site that is visited intentionally or by accident. If you have not installed anti-virus, anti-spyware and other internet security software – stop reading here and go to http://www.symantecstore.com and purchase internet security 2007. This product provides prevention against –

- Fraudulent web sites
- Sending and receiving of email
- Continuous updating
- Firewall protection

I have been using Symantec products since Noah descended from the Ark. Installation and use are easy and yes you need to register the product so that all forms of new malicious codes can be protected against with frequent updates. The current version of Internet Security Suite can be installed on 3 computers. Thus you can use the same product for office and home computers in any combination.

There are lots of other support products including Webroot anti-spyware, McAfee, Panda Software and Zone Alarm.

There will always be bad folks who want to steal what ever you have. When you need more information about these products go to their web sites, ask a professional. The key is take immediate action to protect the computers in the office, at home, on the road.

The last element in this Part 1 is to consider the problems of power needed by computers. When the power stops, laptops can go for a few hours. All other equipment – desktops, servers, telephones, etc. will cease functioning. There are three events that can create power problems:
1. power failure and there is no electricity
This failure can be just in your office or home, in your immediate neighborhood, or in your entire region
2. excess power, called a surge, from events such as lightning
Generally a surge occurs s localized, such as the area surrounding where the lightning strikes
3. intermittent power drops and sudden increase
The local electric utility tries to smooth out the delivery of power but it is not always successful

Answers to the power problems come in small and larger solutions.

Surge protection

Use multi-plug connectors that provide added protection. A terrific product is the powersquid. The Surge 3000 provides terrific design features along with all the built-in power management to protect home and single office environments.

Battery backups

There is a variety of battery backup that are differentiated by the number of minutes or hours of battery power that is provided.

Products from Belkin like this 750VA that enable continuous power for up to 38 minutes. This is not unlimited protection but does provide adequate protection from brownouts and short-term power hiccups.

There are major electric generators that can be obtained as home depot. These require fuel and tend to last less than 24 hours without refilling. New technology from JADOO is at the cutting edge for office and large homes. JADOO uses hydrogen fuel cells, which are replaceable like batteries but have hours of use. While the unit price is high, near $8,000, the capability to protect and office or large home installation is unmatched.

Next Month: Part 2 will discuss security planning and the implementation of appropriate security protections.

About Author:
Richard Oppenheim, CPA.CITP, has used and written about technology for more than four decades. He currently provides advice through the Oppenheim Business Group. He can be reached at richopp@oppenheimgroup.comor through his Web site, http://www.oppenheimgroup.com .