Guiding Principle No. 10: Ensure hardware, software and appropriate patches are in place

Fred Holender, CLU, CPCU, ChFC, MSFS, president-elect of PIANY

We in the insurance business do three things: we help prevent losses; we transfer risk; and we mitigate claims if and when they occur. This month's message is about loss prevention in a world that is active 24/7/365.

Any computer system connected to the internet, or any system that has users, is at risk of a cybersecurity event. Systems and people are vulnerable: we open an email, we click on a link—all seemingly innocent—but the results of these actions can be devastating. In fact, most breaches come from inside, a result of taking the bait set by outsiders who constantly try to invade our systems.

Our goal is to reduce the potential of becoming a victim through proactive loss control. Here are a few tips everyone should incorporate into their routine.

Use hardware and applications that are current and supported by vendors so you receive the latest patches and updates. Many businesses fail to upgrade hardware and software, relying on systems that are at "end of life." These antiquated systems have security holes that are frequently discovered and exploited by hackers. For example, anyone using Windows Server 2003 should know that this version has been unsupported for over a year—there are no patches or updates.

Remember: When you have the latest versions, your vendor will provide customer service for hardware and software. Take advantage of this expertise.

- Use manufacturers' best practices.
- Use the latest versions of Adobe and Java.
- Use the latest versions of your applications provider.
- Use updated drivers.
- Use the latest firmware updates.
- If you have a custom program, make sure you update and install security patches. Some custom programs are obsolete, making them vulnerable to attack.
- Make sure your perimeter hardware, routers and security appliances are up to date. Firewall rules should be current and reviewed on a regular basis.
- Install the most current patches. Have a patch management system. Commit to scheduling updates monthly. If you can't do monthly, make sure you are updating no less than quarterly.
  - Install Windows Update services for your business.
  - Make sure your home computer is set to receive updates automatically.
  - Install security patches.

Cybersecurity is high on national and state priority lists. New York is set to launch new cybersecurity regulations Jan. 1, 2017. To comply, everyone must have an ongoing system management program. Know and understand what you have and where it is located. This is not a "one and done" exercise. System management must become a way of life.

Watch* PIA magazine *for this article and others on cybersecurity in upcoming editions.

Learn more at: nyia.org/guidingprinciples.

PROFESSIONAL INSURANCE AGENTS

iiabny Independent Insurance Agents & Brokers of New York, Inc. Trusted Choice

NYIA New York Insurance Association, Inc.