LTT LAW TECHNOLOGY TODAY

February 15, 2017

CHOOSING THE RIGHT IT MANAGED SERVICES PROVIDER IS CRUCIAL

BY ERIC HOFFMASTER

Has your firm received a security compliance survey from a potential or current client? The answer several years ago was most likely no. Today, however, it is most likely yes.

Information security is one of the top priorities of most organizations today. Securing networks and the data that travels through them is of paramount concern, and rightfully so. From data recovery expenses to potential lawsuits and from the loss of client trust to the hours of patching vulnerabilities, the cost of cleanup after a breach can be astronomical. Taking proactive measures to enhance your firm's security may be costly, but that cost is quickly recovered if even one attempted breach is prevented.

Areas of Cybersecurity

Security is a multifaceted program, constantly evolving and changing. Understanding the various elements is the first step in applying enhanced protections for your firm.

- Infrastructure security – consists of your network and infrastructure devices, such as routers, switches, firewalls, etc.
- Endpoint security – consists of your servers, workstations, laptops and wireless devices.
- Data security – consists of your firm's stored and archived data, including email, file shares, mapped drives, etc.
- Physical security – consists of access to the firm's physical location(s), building, suite and technology rooms.
- User security – consists of your firm's end users, their activities with technology, their email, their passwords, etc.

A properly implemented enhanced security posture requires applying best practices to each of the above areas. Neglect any of them, and your firm will remain vulnerable.

The predominant threat in today's society is social engineering, and it really underscores the need for a 360-degree enhanced security posture. In cybersecurity, social engineering is the act of manipulating people into unknowingly divulging information, allowing hackers access to systems, and it is the most effective and most common way a firm is breached. No matter how secure your environment may be, one password in the wrong hands exposes your entire firm, your data and your clients to risk.

Establishing a security policy for end users and educating and holding them accountable for adhering to the policy form the foundation of a secure system.

Correct Change Required

A new mindset is key when setting up enhanced security: Security requires operational changes. Each one of the facets (infrastructure, endpoint, data, physical or user) requires a change in the way the firm and users operate, and there is often opposition to these changes. “It’s inconvenient,” or, “It slows us down,” are common reactions, and, truth be told, new operating procedures may be inconvenient and may slow the firm and end users down slightly. However, the benefit of enhanced security outweighs the brief delays, and security products are rapidly adjusting to become nimbler, easier to use and more tightly integrated with various platforms.

Change may come in the form of two-factor authentication, requiring your users to enter their network password along with a onetime use token or a request pushed to an approved mobile device asking for login confirmation. This may result in a few extra seconds logging in to a workstation, but the slowdown is minimal compared to the enhanced security it offers.

Implementing enhanced security in your firm isn’t easy. There’s no easy button to apply security or to get your end users to immediately adapt to the change without some resistance. It takes strength of leadership, character and conviction by the firm’s management along with a knowledgeable and experienced team to secure the firm.

Managed Services Providers: A Valuable Resource

Firms of any size have a resource available that can help them understand and implement the necessary changes, educate end users and more. They are called Managed Services Providers, or MSPs. MSPs are external technology services companies that may provide full-service support, consulting services, security services and more. Not all MSPs are created equal, however. With the heightened awareness and focus on security over the last few years, there has been a major push in the MSP industry to offer security services. Many MSPs provide security services, but be careful in selecting the right MSP for the task and your firm.

Selecting a Managed Services Provider

An MSP that has a specialty in, or practice group focused on, security is the first place to start. Find an MSP that knows and actively practices security in its own environment and with clients. Verify its staff has industry-recognized security credentials. Get references from its clients regarding security to establish a track record of success. Focus on MSPs that know your industry, know security compliance

requirements for the industry and can craft a start-to-finish security policy for your firm. Those are the MSPs that understand security best practices and have experience in implementation and support of security protocols. Interview several MSPs and find the fit for your firm.

Once you've established the right fit, get started immediately. After all, the best time to plant a tree was 10 years ago, and the second-best time is right now.

Eric Hoffmaster has worked with Innovative Computing Systems for the past seven years, most recently as the Technical Assistance Center Manager. He can be reached at ehoffmaster@innovativecomp.com.

Originally published February 15, 2017 by ABA Law Technology Today