ALPS
Practice Management Pointers

Are You Suffering from a False Sense of Security with Technology?

Mark Bassingthwaighte, Esq.
mbass@alpsnet.com

We all know that our Internet security programs update on a regular basis and that Microsoft, Apple, Adobe and other software companies release patches with similar frequency. An interesting question is why, and perhaps more importantly, what does it all mean? Truth be told, computer security is something of a reactive defensive play. For example, various Internet security suites defend your computer, mobile device, and network from known and understood cyber-attacks. What about what isn't known or understood? What about the likes of Heartbleed which was an active vulnerability for two years before coming to light?

Here's part of the reality. Once a new banking trojan or other nasty is released by some cybercriminal, the software and computer security companies work on the counter attack, and of course that can only happen after they become aware of the threat. Once they do, these security folk are tasked with determining how the malware works, figuring out how to counter the attack, writing the code that will protect you from this new threat, testing the code to make sure the fix doesn't create other unintended problems, and then they release the patch or update and sit back and wait for all of us to download and install it. In addition to this, the folks who write the software and/or build the hardware we all use day after day periodically release newer versions that often bring with them improved security. By way of example, Windows 10 is more secure than Windows XP just as Internet Explorer 11 is more secure than Internet Explorer 6. Unfortunately, some of us are better than others at following through with installing these updates and staying current with newer versions of the software or hardware we're using. Given this reality, the problem becomes clear. We are all potentially exposed to new and unknown cyber threats until the fix is in.

Yes, most law firms have deployed Internet security software suites, intrusion detection systems, firewalls, and the like and this does make a huge difference. We can and should trust that the efforts of our in-house IT staff or outside IT consultants will keep us safe. Yet this is where the false sense of security comes into play because the real concern is in knowing whether or not these efforts are enough and the answer is no. While IT folks can do quite a bit and their tool box of solutions will continue to get better, a significant vulnerability remains. It is a vulnerability that IT simply cannot control and that vulnerability is us, the people who actually work on the network and use the various computers and mobile devices so many have in play.

As users, our actions can easily and unintentionally circumvent the security tools that have been deployed. What we do with email or the personal devices we bring to the office, where we go on the Internet, the things we download, our social networking activities, the apps we use and where we get them, and even a decision to save our precious data by using public Wi-Fi matters. After all, isn't open public unsecured Wi-Fi is exactly that, unsecured? Just because a signal is there doesn't mean using it is a good idea. Cybercriminals have the same ability to access that signal; and if they have, how would you know they're even there? Now some will say that they're smart enough to avoid most cyber threats but how about everyone else in your office? Are they? Who might be spending personal time browsing the Internet and occasionally disabling the firewall so a page loads properly or who might be using the office's Internet connection to download pirated music or games just for starters?

Is there a solution? Yes, of course. It isn't necessarily easy; but it is manageable and it starts with IT and firm leaders, whoever they are, working together. IT will bring the intellectual capital to the table and firm leaders will need to drive the commitment and follow thru. Part of the solution will lie in periodic and ongoing training in safe practices to include how to identify the many and varied cyber threats. This will need to be ongoing because the attack vectors will continue to evolve and change. Topics such as what is social engineering and how one can be tricked into allowing the computer network to be hacked, why peer-to-peer file sharing networks like the ones that use a BitTorrent protocol can be dangerous, and how can one securely login to the network from a remote location would all be worth discussing.

Personally, I would start with a short session that teaches all attorneys and staff about how the particular security program that IT has installed on your network will respond should an actual threat be detected. Why do this? How many of your users know that if or when a pop-up box suddenly appears informing them that their computer is infected and telling them to click "start scan" is not, in fact, your security software doing its job? Instead, this can be an actual attack. If the user were to click on "start scan," truly believing that this is the right thing to do in order to protect the system, that act will initiate the cyber-attack. If the cyber-attack happens to be a ransomware attack using CryptoLocker, you've got a very serious problem indeed. In December of 2013, ZDNet reported that CryptoLocker, which encrypts your data and holds it ransom until you pay for the decryption key, had been used to procure an estimated 27 million in US dollars from infected users just between October 15 and December 18, 2013!

Another part of the solution will be in establishing and enforcing a firm-wide Internet use policy that spells out the dos and don'ts. Define what might be acceptable to download and what wouldn't. Allowing someone to download an eBook off Amazon might be ok if they were to do it over the noon hour, but their downloading pirated games or music may not be the best of ideas. What about accessing Facebook, Twitter, LinkedIn, Instagram, or Flickr? There are security concerns that come with participation in social media. Do you want to allow access to things like Skype, WeChat, YouTube, or even personal email accounts? In the absence of defined rules, there will be some who will create exposure using such tools solely out of naivety. Don't focus just on the Internet spaces listed here. They are simply examples. All can bring value but all also bring a certain amount of risk. Also try to resist the temptation to just block access to everything because unfortunately there is a catch 22 for many attorneys. For example, blocking all access to Facebook may be a bad idea because there will be times when visiting Facebook will be absolutely called for as part of handling a client's matter. A great resource is available online to assist in the identification of the issues worth addressing in a policy as well as in the development of a specific firm policy or policies. See www.sans.org/security-resources/policies/ for additional information.

The final piece will be in committing to seeing that systems and software remain as current as economically feasible. Windows XP is no longer being supported as an example. While a great program and it will still run, the security updates have stopped coming. Continuing to rely on older software of any type in order to save a little money can be a serious misstep because many malicious programs specifically target older software. Cybercriminals know that the vulnerabilities in these older programs will never be addressed and that works to their advantage. Don’t make it easy for them. Understand that when it comes to computer security, newer and better solutions for hardware and software will continue to enter the marketplace. When you think about what is at stake, isn’t the investment cost of updating to the most current version of a software program available well worth it? I certainly think so.

Risk Management Questions?

Mark Bassingthwaighte, Esq. is the Risk Manager for ALPS Property & Casualty Insurance Company. He is available to answer risk management questions and can be reached at 1-800-367-2577 or mbass@alpsnet.com.

Disclaimer:

ALPS presents this publication or document as general information only. While ALPS strives to provide accurate information, ALPS expressly disclaims any guarantee or assurance that this publication or document is complete or accurate. Therefore, in providing this publication or document, ALPS expressly disclaims any warranty of any kind, whether express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

Further, by making this publication or document available, ALPS is not rendering legal or other professional advice or services and this publication or document should not be relied upon as a substitute for such legal or other professional advice or services. ALPS warns that this publication or document should not be used or relied upon as a basis for any decision or action that may affect your professional practice, business or personal affairs. Instead, ALPS highly recommend that you consult an attorney or other professional before making any decisions regarding the subject matter of this publication or document. ALPS Corporation, as well as any of its subsidiaries, affiliates and related entities shall not be responsible for any loss or damage sustained by any person who uses or relies upon the publication or document presented herein.