ALPS
Practice Management Pointers

Cyber Crime: Why Your Ignorance is Their Power.

Mark Bassingthwaighte, Esq.
mbass@alpsnet.com

The title to this article explains the real problem when it comes to cyber security. Regardless of all the precautions you or your IT support have taken, from steps like securing your digital assets with the latest and greatest in firewalls and antivirus software to upgrading to the latest in browser software or operating system, those efforts still aren't going to be good enough. There is a weak spot that IT support can't easily address and you can't fix by throwing a little more money at it. The true vulnerability comes from the folks who use your systems. I'm talking about you, your partners, your associates, your staff, and anyone else who has access to or uses a firm computer, tablet, smartphone, and the like. How do you think the Target breach, and all the other ones we hear about with ever more frequency, happened? In short, someone did something stupid like opening an email, clicking on a link, or verifying a password because he or she didn't know any better or they got caught off guard.

To help bring the point home, ask yourself these few questions and focus not only on how well you can answer them **but also think about how everyone else in the office might do**. Do you know what CryptoWall and Neverquest are? (CryptoWall is ransomware that encrypts files on every drive it has access to and Neverquest is a banking Trojan.) If you did know what these two examples of computer malware were, do you know if you can still be infected by either if you have an Internet security software suite running? (Yes, until a patch is released for each new variant that is discovered in the wild; but be aware that malware is rapidly moving into the mobile space where many are woefully unsecure.) Can a computer attack start with a simple phone call? (Yes, it's called a phishing phone call.) What is spear phishing? (Targeted attacks that appear to come from a trusted source.) Can identity theft occur via a text message? (You bet.)

Hopefully you start to see my point. As users, our actions can unintentionally circumvent the security tools that have been deployed and often it happens out of sheer naivety. Someone is uninformed and a cybercrime can occur as a result. What any of us do on the Internet and even how and where we do it matters. For example, unsecured Wi-Fi is exactly that, unsecured. Just because a signal is available doesn't mean using it is a good idea. Cybercriminals have the same ability to access that signal as you do and how would you know they're there waiting for you? Again, perhaps you are smart enough to avoid most attacks but how about everyone else in your office? Do you know what they are doing online or with their mobile devices?

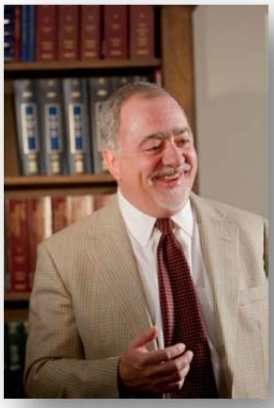
So what's the solution? How does one address the very real threat that comes from each and every user? I wish it were easy. Unfortunately, it isn't; but it is manageable. This is one of those situations where IT and you need to work together. Part of the solution will lie in periodic training in safe practices to include how to identify threats. This needs 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 into the network from a remote location would all be worth discussing. Personally, I would start with a short session that teaches everyone about how the particular security program that you run on your network will respond should an actual threat be detected. What will that look like to the user and what should they do if it happens? Why do this? How many of your users know that if and when a pop-up box suddenly appears informing them that their computer is infected and telling them to click "yes" in order to start a scan is not, in fact, your security software doing its job? Instead, this can be an actual attack by the likes of CryptoWall. If the user actually clicks on "yes," truly believing that this is the right thing to do in order to protect the system, that act will initiate the malicious program. Trust me, with CryptoWall that's not what you want to have happen.

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 downloading free stuff along the lines of screen savers, emoticon programs, desktop wallpaper, and even music may not be the best idea. What about accessing Facebook, LinkedIn, or Pinterest from an office device? There are security concerns that come with participation in social media. Do you want to allow access to things like Skype, Instant Messenger, YouTube, or even personal email accounts? In the absence of defined rules, there will be some who will expose the network if for no other reason than through naivety. Also, 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.

Again, there is no easy solution, and unfortunately there is a catch 22 for many attorneys. For example, there is often a temptation to simply block access to something like Facebook; but this may be a bad idea. For some lawyers there will be times when visiting Facebook will be

absolutely called for as part of competently handling a client's matter. The good news is that a great resource is available online to assist in the identification of the issues as well as in the development of a firm policy or policies. For additional information see www.sans.org/security-resources/policies/.

The final piece will be in committing to seeing that systems and software remain as current as economically feasible. Why? If you have an older version of a program still in use at your office do you know if it is still being supported? As newer and more secure versions of software come to market, software companies eventually stop supporting the older versions. Now this doesn't mean the program stops working; but it does mean the security updates stop coming. Continuing to rely on older software in order to save a little money is a serious misstep because many malicious programs specifically target older software. Cybercriminals know that the vulnerabilities that still exist in these older programs, for example Windows XP, 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?



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.