BE WARY OF CYBER THREATS

December 20, 2017

By: Darryl J. Horowitt

If you run a company that uses computers that are accessible to the Internet, cyber security should be important to you because of the importance of preserving the confidential information in your computer system. What is cyber security? Simply stated, it relates to the preservation of electronically stored information and preventing attacks from third parties who want to take the confidential and personal information from you and sell it to others as part of a criminal enterprise. These attempts include phishing, attempts to hack into your system, and ransomware that encrypts your computer so that the information is not accessible unless you pay a ransom.

There are, of course, more threats, but the above gives you an indication as to some of the more common threats that your business faces every day. Numerous articles can be found on the Internet that outline how you can protect your company's computers. Common sense steps include:

1. Require passwords to log onto your computers and change the passwords every 60 days. Having a two-step authentication process is even better.
2. Do not leave passwords in the open or where they can be accessed by third parties.
3. Update your operating software and program software. It appears that the WannaCry ransomware attack exploited a software flaw in Windows 7, a version of the Windows operating system that was not being supported by Microsoft. Those who suffered from attacks might have avoided that fate if they had updated to a newer version of Windows that was supported by Microsoft.
4. Update your anti-virus software regularly and, if possible, erect a firewall that will identify and stop potentially threatening e-mails from being delivered in the first place.
5. Train your employees to spot potentially harmful e-mails including: an e-mail that is either sent to a number of different recipients or where no recipient is identified in the "to" line and contains only a link; an e-mail from either a known or unknown source that states you have documents being sent to you and provides a link, but no requests for documents have been made; an e-mail sent by a bank you may or may not work with that asks you to verify your information – most banks will not ask you for that information and will contact you in other ways to do so; a company

you work with asks you for your financial information even though it is not necessary to complete a transaction or it has already been provided to those who need the information; an e-mail asks you for your Social Security number even though by law it cannot be used for identification purposes and generally should not be provided to any third party for any reason (if they need the information, give the last four digits only to match up with information they already have); and any other e-mail that just looks funny, in which event you should ask your IT provider to check to see if it is a legitimate e-mail that can be accessed. Training should be continuous and ongoing because new threats arise on a regular basis.

6. Have your IT provider regularly review your system and test it to make sure that it is not vulnerable from outside sources.

7. Consider buying cyber security insurance coverage. Like any insurance, it is an expense and many cash-strapped companies put it at Fresno | Los Angeles | Bakersfield | Visalia | Sacramento Representing Businesses and Their Owners the bottom of their list. Unfortunately, however, you just need one cyber attack to cripple your company and expose it to tens of thousands, if not hundreds of thousands, of dollars in potential damages. Further, as businesses you work with get more sophisticated, they will want to see that you have cyber security coverage.

As a firm, we understand that it is important for us to keep our clients' information confidential and implement the above policies. We have also instituted additional steps to assure that our clients' confidential information remains confidential. We have updated our on-site security and we do carry cyber security insurance. Our IT supplier regularly updates our computer system to minimize the potential of a cyber attack. You can rest assured that we will continue to take steps to preserve the confidentiality of your information. We urge your company to do so as well. It is no longer an option to wait and hope nothing happens.

This article was written by Darryl J. Horowitt. Darryl is the managing partner at Coleman & Horowitt, LLP, where he works in the firm's litigation department and represents clients in complex business, construction, banking and real estate litigation, consumer finance litigation, commercial collections, casualty insurance defense, insurance coverage, and alternative dispute resolution. He has been named a Northern California Super Lawyer® (Thomson Reuters) in business litigation from 2006-2020, a Top 100 Northern California Super Lawyer® (Thomson Reuters) from 2015-2019, has received an AV®-Preeminent

rating from Martindale-Hubbell and a perfect 10.0 rating from Avvo. He is a member of the Fresno County, Los Angeles County and American Bar Associations, the Association of Business Trial Lawyers (former President and Board Member). Darryl can be reached at dhorowitt@ch-law.com or (559) 248-4820, ext. 111.