CYBERSECURITY AND THE REAL ESTATE AGENT

The Marriott Corporation just announced that hackers stole information on as many as 500 million guests over a four year period, obtaining credit card and passport numbers and other personal data. This is clearly one of the biggest data breaches in history. In 2017 the Equifax breach affected more than 145 million people. A Target Corp. breach in 2013 affected more than 41 million payment card accounts and exposed contact information for more than 60 million customers and the number of companies who have become targets is increasing at an alarming rate. Clearly this type of crime has become the new norm in our society and as a result, it is no longer a question of "if" you become a victim, it is now a question of "when" your office systems are disabled as a result of these "cyber-criminals."

Our industry relies heavily upon technology since real estate firms are creating, using, storing and sharing more and more personal and sensitive information on clients and customers. As we embrace a paperless environment, we have become dependent on online information storage vendors or in many cases, the information is stored on proprietary servers in the office or in remote locations. Rental and coop/condo board applications, contracts of sale, closing disclosures, lease and rental agreements, financial information and credit reports all contain personal information which is a treasure trove for hackers who sell the stolen data to other cyber-criminals on the dark web. Risks can exist in many forms from malicious cyber-attacks, to negligent employees or agents, to unmanaged data sharing with vendors; therefore, real estate professionals must take a serious look at their cyber risk exposures and how they are managed.

Ransomware, malware that encrypts data on computers and makes the data unavailable until a ransom is paid, has become an immensely profitable method for hackers to attack businesses. Like most companies, real estate businesses rely on electronic information and systems to run day-to-day operations. An employee or agent clicking on one malicious email can lock up the information for the entire company. With the advent of home and office security systems that are internet-enabled, lights can be turned on remotely, doors can be opened and locked and thermostats and other physical based devices can be activated at the touch of a key stroke. This same technology that allows us ease of use brings with it an increased risk that hackers can take control of those systems or make the systems unworkable.

While ransomware has become the method of choice of cyber-criminals, real estate professionals including brokers, agents and attorneys have been targets of hackers who attempt to obtain banking credentials or personally identifiable information. A real estate transaction concerning the sale of property can take approximately two to three months from contract to closing. During this period, cyber-criminals who are able to place a "Trojan horse" into the computer system of one of the participants to the transaction patiently waits until a closing is scheduled before masquerading as an interested party.

When one of the attorneys or real estate agents provide wiring information to his or her clients, the cyber-criminal monitors this communication and sends another email to the recipient which modifies the initial wiring instruction in an attempt to capture the victim's banking credentials and wipe the bank account clean.

The National Association of Realtors recommends that real estate professionals always take preventative measures, especially when it comes to wiring transactions, such as communicating with clients before a transaction about the possible dangers of wiring funds, to call the intended recipients of wired funds before sending them and to always independently verify phone numbers associated with a wiring transaction. In addition, something as simple as securing accounts with strong passwords can help reduce your risk of becoming a victim. In the event funds are mistakenly wired to the wrong account because of the successful efforts of cyber-criminals, the local FBI office should be immediately notified and in many instances, procedures can be undertaken to recoup those funds before they actually are deposited into the criminal's account. In addition, real estate firms and attorneys can obtain cybersecurity insurance to assist if and when the firm's computer systems are held hostage or monies are improperly removed from bank accounts. Cyber insurance covers expenses to retain a computer forensics firm to determine the scope of a breach, to comply with privacy regulations by notifying your clients and customers of the data breach, to notify and provide credit monitoring services to restore the company's reputation, to recreate the data due to a network security failure and surprisingly, it also covers extortion monies and associated expenses arising out of a criminal threat to release sensitive information or to completely shut down a computer network.

This article is not meant to address all the precautions that can be taken to reduce the risk of a computer or systems breach. It is recommended that you speak with your IT professional and/or insurance carrier to explore the ways you can help to protect yourself if that day comes (and it almost certainly will come) when you sit at your desk and read that your files or accounts have been hijacked by a cyber-criminal…so direct yourself accordingly.

Submitted by Alfred M. Fazio, Esq. of Capuder Fazio Giacoia LLP. Visit our website at CFGNY.com for copies of recent articles as well as other areas of interest to the real estate community. If you would like to be added to our mailing list and receive future articles, please click the link below.
http://visitor.r20.constantcontact.com/d.jsp?llr=qgisqkiab&p=oi&m=1108454482128