Take measures to prevent cyber breaches - by Joseph Saracino

October 06, 2020 - Long Island

Joseph Saracino

October is cyber security month and an excellent time for members of the real estate industry to review their current cyber security plan and take important steps to protect against cyber breaches. According to a KPMG report, over 50% of real estate businesses are not prepared for preventing a cyber attack. Given the increase in hackers targeting of real estate businesses, it's important that companies across the industry, from brokers, agents, real estate finance firms, title companies, property managers, etc. implement a sound cyber security plan encompassing education, vigilance and best practices.

First and foremost, companies need to heighten the awareness of all staff, educating them about common cyber threats and how to identify them. There has been a steady increase in phishing, social engineering, ransomware and keystroke attacks. Staff should be taught what to do and not to do and how to identify the top malicious email attachments which include .doc, .dot and .exe and directed not to open them unless the email is from a known sender.

Keep in mind that cyber criminals target companies in certain industries in similar ways. They are particularly active targeting organizations handling a lot of financial and personal data. It's easy to understand then why financial institutions, credit card companies, healthcare, and real estate companies would be prime targets. A majority of cyber attacks have a financial motivation resulting in widespread theft of bank account, credit card information and Social Security numbers. In 2019, 62% of all businesses experienced phishing and social engineering attacks with 71% of those attacks financial motivated.

Cyber criminals attack every 39 seconds, on average 2,244 times a day and, the average time it takes to identify a breach is 314 days. You can see how much damage can be done in that time. From January to June 2019, cyber breaches exposed 4.1 billion records with the average costs of a breach in 2019 at $3.92 million. The stakes are very high.

Compliance to cyber security regulations is an integral component of a sound cyber security plan.

There are non-industry specific laws such as the General Data Protection Regulation (GDPR) of the European Union (EU) governing data protection and privacy in the EU and the European Economic Area (EEA), as well as the transfer of personal data outside the EU and EEA areas. Additionally, there are state laws, such as the New York SHIELD Act. It expanded the types of “private information” that can trigger data breach notifications, and requires businesses and individuals to take certain preventive measures to protect the data they own or license. Other regulations are more industry-oriented such as the New York State Department of Financial Services’ Cybersecurity Regulation, Part 500 of Title 23 of the New York Codes, Rules and Regulations. This regulation made headlines recently when its first enforcement action was reported against First American Title Insurance. First American Title was charged with exposing millions of documents with consumers’ personal (non-public) information including bank account numbers, mortgage and tax records, Social Security numbers, wire transaction receipts, and drivers’ license images. Had First American Title adopted and implemented best practices in cyber security it is likely the company could have prevented those data breaches. Instead, First American now faces six provision violations to be taken up at a hearing in October. Based on the outcome of that hearing, the company might have to pay penalties of up to $1,000 per violation and an additional penalty of up to $1,000 per violation of non-
public information exposure.

To ensure a sound cyber security plan, it is advisable that real estate organizations have regular vulnerability assessments and penetration tests on their networks conducted by a third-party cyber security firm. Having the in-house IT department or your managed service provider conduct these tasks is not sufficient and does not provide the essential check and balance a third-party provider can. Also essential is to have a comprehensive cyber security manual which clearly outlines all policies and procedures that staff and any vendor with access to the business IT systems and network must follow. The manual should include best practices, e.g., avoid and do not open pop-ups, unknown emails and links, create strong passwords and change frequently, multi-factor authentication, connect only through secure WiFi, and maintain up-to-date security software. It is also important to consider new technologies that help detect and mitigate cyber threats.

When it comes to cyber attacks, it’s not a matter of if, but when. Avoid being a victim and subject to the losses–both financial and reputational–you can incur as a result of a lax cyber security plan.

Joseph Saracino, president and CEO of Cino Ltd., Jericho, N.Y.