THE REGISTRY
BAY AREA REAL ESTATE

October 19, 2017

Should Landlords Conduct Cybersecurity Audits?

By Christian Leitner

A recent KPMG survey of businesses in the real estate industry showed that about 50% of surveyed organizations believed that they were not adequately prepared for a cyberattack. Currently no federal law is requiring real estate businesses to implement and maintain information technology security programs. This led to an industry-wide increase in system vulnerability.

General IT threats targeting organizations across many different industries are emerging in an alarming rate. Business email compromise (BEC), Ransomware and other Malware attacks cost American businesses billions of dollars last year. Furthermore this is all aggregated by the trend of cloud computing applications, which also have been heavily adopted by many real estate businesses.

For example property management and lease administration systems, have become a lucrative target for cybercriminals. These systems usually contain personal information of tenants and are also used for cash transactions.

The Internet of Things (IoT), which is starting to play an important role within the real estate sector in the form of smart “connected” buildings, new security technology based on wireless technology and biometrical security access systems and sensors, like face recognition and finger print scanning, opened up new vulnerabilities prone to hacking. These threats were also mentioned by Deloitte as an increasing area of potential attacks and an evolving cyber risk in commercial real estate.

Cybersecurity is no longer a topic discussed during IT meetings, it has now become a business conversation. More and more board and audit committee members across the nation view cybersecurity and loss of company reputation as a major risk that will need to be paid more attention to in the near future.
In order to do this, board members and owners should get involved and ask security professionals within their organizations the following questions:

- Do we have a wire policy that will protect us from BEC?
- Are all our critical systems backed up on a regular basis to restore data potentially compromised by Ransomware or Malware?
- How do we select and evaluate cloud service providers? Are SOC reports available?
- How would we respond to an incident or breach? Do we have an incident response plan?
- Is it documented? When was it last tested?
- Have we considered cyber liability insurance?

In May 2017, The American Institute of CPAs (AICPA) released their long awaited Cybersecurity Attestation Framework (CAF). Also known as Service Organization Control(SOC) for cybersecurity, this framework builds on top of the long established Trust Services Principles (TSPs)reporting. TSPs are the underlying criteria for SOC reports, but were usually limited to one or more systems delivering services to an organization’s customers. The newly released CAF uses these TSPs but applies them across an entire organization instead of just a specific system or department. In what could be seen as “SOC reporting on steroids,” the scope is much larger and covers all aspects of an organization’s cybersecurity program. The purpose of such an attestation is to deliver an independent evaluation by a Certified Public Accountant (CPA)registered and in good standing with the AICPA. CPAs are in the unique position to perform these audits given the AICPA standards, which are available to the public and whose scope is the same for every organization. Many CPAs are currently promoting this as a separate service line to be performed annually or semi-annually.

The application of the reports could make it a vital tool in the future regarding how to deal with cybersecurity questions related to your own organization, your customers and other third parties identified

during your risk assessment. The independence factor will move this approach above the existing self-monitoring and self-assessment reports given to stakeholders. For example, the customer will get the report addressing the effectiveness of its cybersecurity program according to the TSPs and can then use it to show internal (e.g., board members, audit committees, owners) or external (e.g., customers, third-party contractors) stakeholders that their program can be relied upon.

While the CAF is still in its adoption phase, it received a lot of positive feedback prior to its release in May from early adopters and professionals in the cybersecurity field. The general consensus is that the CAF will open new ways for organizations across the U.S. to deal with cybersecurity questions and helpevaluate internal and external cybersecurity risks from a business perspective.

Christian Leitner is a Certified Information Systems Auditor (CISA) with more than 10 years of experience in all aspects of technology infrastructure and compliance. He has been leading Sarbanes-Oxley IT audits, SSAE16 SOC1/SOC2/SOC3 engagements and other IS compliance consulting projects since 2004. He also has in-depth knowledge of hardware and software implementations, business process analysis and redesign, IT project management, IT risk advisory services, disaster recovery and business continuity planning. He can be reached at cleitner@oumcpa.com.