Systems Security in 2017

It appears that the term cyber security has hit new highs of awareness and it's presence in the media. Yahoo and its millions of users has been hacked. Wiki link and its data releases have been active with its files related to the DNC and the election. Ransom ware has been activated in a few hospitals resulting in acts of extortion. At least one hacking of a power grid has taken place recently.

All of the above indicate the potential of a security threat on your property management system and its data. The preponderance of media stories however, are focused on large agencies and organizations. According to one cyber security expert one or more online property management systems also has been hacked . The property management industry in general is not the target size of Microsoft, Google, Face book and many others, but it it is a "target rich" environment.

An on-line system generally entails the portfolios/ databases of multiple companies and their owners and tenants including bank accounts, social Security numbers and other confidential data associated with identity theft and monetary value. Generally, the servers and PC's working with these databases are well secured. The threat however, is more obvious with the growing number of remote and mobile devices supporting systems operations.

Recently I attended a cyber security presentation sponsored by the San Diego Association of Realtors, (SDAR). It was indicated that there are data breaches not generally published or in some cases even known. It was indicated that some real estate oriented breaches including brokerage and escrow operations have resulted in large wire transfer losses. According to the one cyber security expert one or more online property management systems also have been hacked. He may gace been referring to AirBNB which was hacked in October along with Amazon and a number of other large companies.

It was also indicated that another major security issue is the increasing property management systems operations involving remote location and mobile devices especially with laptops, tablets and smart phones. See WiFi below.

On-line systems use the Internet continuously based on the remote location of the servers providing both the program and data to the users at locations that may be hundreds of miles distant from the servers. This is less true of standalone system which may periodically use the internet for support operations such as background checking and ACH/ EFT operations. Generally, standalone systems are operating in a single location with the possible addition of one or two users working off of their office system remotely. That accommodation is possible with communication software such as Remote Desktop Protocol, Go To My PC, Log Me In, etc.

Companies using standalone systems, that is servers or PC's in the company office hosting the program and the data, are also subject to data breeches and losses, but with much smaller losses based more often on embezzlement, theft and small conspiracies. Vendors and tenants may conspire with staff involving rent charges and payments, materials and services. Having 30 years plus of property management systems experience I am aware of numerous losses based on those criminal activities, but are not aware of any hacking losses with standalone systems yet.

An additional element of system security relating to both standalone and on-line systems is the Red Flag Rule. The Red Flags Rule requires most businesses and organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs – or red flags – of identity theft in their day-to-day operations. The Federal Trade Commission (FTC) is the government agency sponsoring the rule. Inadequate procedures related to confidential handling of personal data such as tenant prospect background checking procedures may result in a Red Flag Rule violation.

Residents managers, leasing agents, property managers and maintenance staff are increasing their ongoing access to the system and the data they require by transitioning to on-line systems and the various remote and mobile routine using laptops, tablets, and smart phones. Mobile routines are likely to access the system and the Internet using Wi-Fi "Hot Spots".

According to the cyber security specialist the use of the above devices in the field is where the additional threats are active. Based on their use in the field the additional potential of theft, loss and damage while in the field are omnipresent. In some cases using Wi-Fi hotspots available in hotels coffees coffee shops airports etc. can be a benefit but is not always a secure or generally secure facility. Wi-Fi hotspots provide Internet access in public locations, but unfortunately too often the Wi-Fi is assumed to be as secure as an office system, but is not. Note the recommendations at the end of this document.

Generally a secure WiFi hotspot will require a password. Other security settings may be seen by hovering your mouse over each WiFi connection in your WiFi settings. WPA2, WPAand WEP are 3 types of secured connections. It is likely that acceptance of the terms of use agreement will be required before connection. Wi-Fi locations should be checked for current security acceptability.

Note: Cox Communications provides many secure local Wi-Fi in the San Diego area. The WiFi hotspot can be used both by Cox customers and non-customers (with a local free trial). Cox Communications has more than 1,000 WiFi hotspots in San Diego County available to Cox customers and non-customers. Non customers can access the Cox hotspots through a free one hour trial. Cox customers can just find Cox WiFi or CableWiFi in their WiFi settings. " WiFi Hotspots 101 – La Mesa Courier" November 2016"

Recently a new security threat was demonstrated on a CNBC program involving public charging stations. Certain components of the stations allow the station to be activated as a video camera providing video of the individual using the charging service and their activities while their device is being charged. Obviously certain activities , on-line banking, on-line purchases, etc. are major opportunities for the criminal hacker.

The following are key recommendations regarding system security.

- Every system user should have their own user ID and password using a combination of mixed character's, I. E. upper and lower case, numbers and symbols, in addition to only having access functions that are part of their assigned responsibilities.
- In addition they also require password access for its their device and the property management system / application.
- IT staff or vendor should periodically test system for malware and current security software.
- A relatively new security threat is that of public charging stations, A recent radio announcementand a CNBC program indicated that hackers have managed to utilize some of the components in the charging station to create videos of the user and their device operations. activate some This is a new technique to spy on the activities and operations of a Smartphone user. public charging stations as a means tu hack the users device.
- Finally, the user must remember they may be in a very public place where they may be observed by a hacker who is primarily there for the potential of criminal activities they can perform. Personal activities such as on-line bank operation, and credit card purchases are not recommended in WiFi hotspots.

Dick Jonilonis 619-460-8925 dickj@pmsoftwaresolutions.net www.pmsoftwaresolutions.net

February 2017

DJ&A
DICK JONILONIS & ASSOCIATES