nerej
CELEBRATING 55 YEARS

Cybersecurity - Hackers: Coming soon to a building near you - by Jonathan Avery

October 30, 2015 - Front Section

Jonathan Avery, Avery Associates

Cybersecurity is all over the news today as a major concern with significant impacts to our economy. Attending a program at the recently concluded Counselors of Real Estate (CRE) Conference is Charlotte, NC, the local and immediate impact of cyber threats came through clearly. As we are

increasingly becoming aware, building management, maintenance and control systems are increasingly online. Everything from HVAC systems, security access, environmental controls/energy management, garage access systems and wireless networks are potential entry points for hackers to attack. The impact of these threats on real estate can be disastrous. For example, few realize that installation procedures developed by building equipment manufacturers, in more than 50% of the cases, include use of generic passcodes and logins for security access. These generic passwords are available easily through an Internet search identifying the equipment and manufacturer. So, if you do not change the access procedures and passcodes at the time of installation, these systems may provide an open backdoor for a cyber-attack. Cyber-attacks can come in many variations. A frequently described method of attack is called “theft of buildings.” In this type of attack, a hacker will gain access to building management systems such as lighting or HVAC and shut down the entire building. An email will arrive detailing the ransom to be paid in order to return control of the building. However, this is the point at which building owners and managers should immediately contact law enforcement officials since continued blackmail is often the pattern.

Data theft through access to management information systems, either of tenants or building owners, is another form of attack. Personal identification information may be hacked as a result of access through an unprotected wireless network or even through remote control building management systems. Often these attacks may not be immediately apparent. Once access is gained into the building information systems, an attacker might use this as a springboard to proceed through related networks and this initial attack becomes a force multiplier with the potential to cause severe havoc. These and many other examples certainly gained the attention of all the participants in this workshop. The next logical step is to develop a plan to protect both building owners/managers and tenants within the building.

In addition to the above-noted example of default passwords and logins on equipment, many times operators lack awareness of the soft points in cybersecurity. Some of these soft points include third party vendors, client contract obligations or even something as simple as an online procedure for maintenance and repair requests. All of these can be paths into the systems of building owners and users who perceive their core to be secure.

Increasingly, the “Internet of Things” may be an “Internet of Insecure Things.” It is entirely possible that remote control thermostats, LED lighting control systems and something as simple as smart phone access to your desktop computer are all potential open doors for cyber-attacks. The downside of a successful cyberattack can be devastating. Not only loss of use, which may be temporary, but also repair of any damage and identifying the source and providing secure protection may be needed. These are all time consuming and expensive. In addition, liability for loss of data can have a severe financial result. Further, regulatory and government monitoring is increasingly widespread and can result in fines or other punitive action for not providing proper protection to critical infrastructure.

Protection can be provided by a combination of things. First, a thorough review of your cybersecurity from a technical and regulatory standpoint is a must. Insurance is becoming increasingly available to protect this risk, although care must be taken that you have the protection that is specific to your needs. Completing a periodic audit of all systems can be an important deterrent. This is a real threat to building owners and managers and will increasingly affect the design, construction and operation of buildings in the future. Caution and thorough preparedness are the prevent defense.

Jonathan Avery, MAI, CRE, is president of Avery Associates, Acton, Mass.