Cyber Threats

By
Marc Petock
Vice President, Marketing
Lynxspring, Inc.

We are experiencing a reality check. Today's reality is this: No matter what business you are in, no matter where in the world you are—everything on a network is at risk.

Cyber threats and security compromises directed at building and facility control systems remain one of the most dynamic issues in the building automation industry today. Buildings are highly susceptible to cyber threats, hacking and viruses.We have seen the number of cyber related incidents and discoveries of building automation software vulnerabilities ramp up. Cyber threats within the building environment are becoming more frequent and sophisticated and we are now at a point where we should be concerned. Gone are the days of "security through obscurity".

Like enterprise computing, building control systems have traveled a path from standalone systems to the modern, highly interconnected world of Ethernet, the Internet and cloud-based computing.We have spent years developing building control systems and smart building automation systems that are interoperable, are accessible from anywhere at any time and easy to use. Attributes like openness, ease of connectivity, real-time, greater levels of control, increased operational efficiency and effective service are the same ones that now make these systems vulnerable to viruses, subject to attacks, unauthorized access and breaches.

As these systems have become more and more interconnected and we extended the connectivity of these systems to external networks, brought intelligent buildings to life, realized our buildings are business assets and the data contained in the devices is valuable and increased the use of enterprise software platforms and applications (which has brought huge benefits), these systems have now been introduced to cyber security concerns and are targets to threats and risks.

It is not just about being able to turn the lights on or off or raising or lowering the temperature a degree or two. Characterizing possible disruptions to lighting or HVAC controls as a little harmless mischief dramatically underestimates the value of these systems to productivity, safety and the overall bottom line for a business. I am reminded of some examples shared with me recently. What if a building automation system was breached through cyber means and it caused the building's sprinklers and smoke alarms to fail; or disabled the elevators in a multi-story building —all of which could have potentially serious consequences should a fire break out. How about a person or persons penetrating a building's access controls system and allowing unauthorized entry or preventing occupants from exiting. Even causing the failure or inoperability of the HVAC system could have detrimental consequences such as causing temperatures to stray outside acceptable limits, the building could become inhabitable for the occupants, damage equipment through excessive temperatures, or result in damage to materials.

Building Automation Systems are increasingly incorporated into computer networks. If someone hacks the BAS system, they now have an attack vector into the company network. A hacked device can become a pivot point that can bypass many existing network defenses. Today, a hacker can use a BAS device as a jumping off point onto other devices and computers on the network, and because they are coming from a trusted device – inside the network – traditional network security can ignore them. Employee records, customer data, intellectual property are now more vulnerable.

The negative consequences and potential risks cyber incidents can cause are multiple. From impacting occupants directly, to businesses and operation disruption, to employee productivity, to accessibility, to downtime, damages can include interruption of key services, a shutdown of business operations, exposure and compromise of sensitive information and damage to physical equipment and the building itself and even loss of life. And then there are the monetary and social consequences of a breach such as negative publicity, loss of customer confidence, impact to reputations (company and personal), potential lawsuits, and direct financial loss caused by interruptions and equipment replacement and repair. And if you are a building owner relying on tenants, you risk losing them.

From the outside in, to the inside out, threats are increasing as quickly as you can implement measures against them. While we do have cyber security mechanisms that address some of the risks, including password access and requirements, VPN's, firewalls and software patches when made available from providers, are these enough to prevent unauthorized and malicious activity?

The best way to approach cyber threats is to realize one simple truth: It is not if an attack will happen; it is only when. Successful cyber threat prevention involves multiple paths of defense and layers of protection. Yes, we need to build secure building networks with Firewalls and VPN's but it also requires strengthening the cyber security posture of automation control systems with security and pre-emptive threat protection for the devices and systems across a building network by securing, managing, controlling, tracking and monitoring all account access and activities.

It is making sure devices that fall outside the scope of traditional remote access solutions are secure. It is constructing security zones to protect groups of devices and systems and restricting access and permissions and preventing the exploitation of local or remote access to privileged accounts. It is performing audits by recording user access, timestamps and actions taken.

A comprehensive cyber security program leverages industry standards and best practices to protect systems and detect potential problems, along with processes to understand current threats and enable timely response and recovery.

Cyber related issues play a growing role within our building networks. Building automation systems are highly susceptible to cyber-attacks. They are not immune to attacks. Don't underestimate the potential for cyber vulnerabilities. It only takes one single breach to compromise the whole infrastructure and cause a serious issue.

It is not just the responsibility of one group; it is everyone in this industry. Technology providers need to incorporate security features and functions into their technology; system integrators by way of best practices, should secure their installations using IT security practices and end users should demand and insist on protection from cyber threats.