Fire Protection Systems and Cybersecurity

With the ever-growing importance placed on technology in our everyday lives, fire protection systems are no exception. In the last 10 years, fire protection technology has become increasingly integrated with building utility infrastructure allowing for functionality, ease of access and greater control. However, as is often the case with technology, the convenience and efficiency of these integrations may come with hidden risks.

Cyberattacks are becoming a common occurrence in our modern world. Targets can range from personal computers to corporate servers to water management systems. It should come as no surprise that fire protection systems installed within commercial buildings are no different. As fire protection systems are becoming increasingly sophisticated so are the integrations with building automation systems. Current fire protection systems could have potential access to HVAC systems, elevators, CCTV and generators. Perhaps most concerning are the systems with direct access to the internet. Without the proper protections this gateway could allow outside access to anyone with sophisticated enough technical knowledge and skills.

So why are these systems being targeted? Who would want access to a building's HVAC equipment? Tyler Robinson, an ethical hacker, and owner of the company, Dark Element says, "Building systems have traditionally been one of those areas that is often ignored." This is referring to the sometimes-lax attitude surrounding cybersecurity when it comes to building utilities. The Programmable Logic Controller (PLC) software or OS can become outdated, the hardware can require important security updates which remain uninstalled. Even the physical area itself might not be heavily scrutinized. Tyler recalls a situation in which, for training and education purposes of the organization he was hired to pose as an elevator technician to perform an annual review inspection. Tyler was given full run of an elevator utility area complete with access to a computer. This scenario would be more than enough of an opportunity for a hacker to attempt to infiltrate the system through the elevator software or by using the computer and gain access to the corporate server.[1]

Once access to these IT systems is granted there are a variety of potential issues that could occur. Most commonly a hacker or "adversary" can encrypt the systems making them unusable and require a ransom to unlock it. This is referred to as "ransomware." However, within building automation something much more unique could be a threat. As control over these systems are also kinetic they can affect elements within the physical space of the building. This can present a multitude of different problems completely separate from the cyber-physical world. In some situations, the ability to affect the building on a physical level could put the occupant's well-being at risk. This is especially true for the more vulnerable occupancies such as hospitals and elder care facilities. Within these buildings homeostasis is in such delicate balance that loss of control over an elevator, HVAC system or sprinkler system could cripple them to the point that an evacuation would be required.

So what can we do? Training and education must be at the forefront. Any organization that utilizes IT systems needs to have a strict protocol of procedures that is followed by every employee to help keep the systems secure. This includes vetting anyone that intends to enter the secure areas of the building by calling the company they claim to work for. IT staff need to ensure that not only computers and servers receive constant checks and updates, but any systems within the building connected with the mainframe or the IOT (Internet of Things) are monitored as well. Companies need to practice good "cyber hygiene" which means keeping software up to date, replacing unmaintained hardware and being aware of and monitoring system norms. They say a chain is only as strong as its weakest link. In taking inspiration from this wisdom, organizations should feel encouraged to test the limitations of their IT preparedness and hire an organization that specializes in cybersecurity and ethical hacking that will attempt to penetrate building security either through the internet or directly in the real world.

It is becoming increasingly apparent that security surrounding fire protection systems should be treated with top priority. As time goes on this technology is only going to become more elaborate and interconnected with building

[1] Cybersecurity for Fire Protection Systems: A Panel Discussion: https://www.nfpa.org/Training-and-Events/By-type/Webinars
https://www.nfpa.org/News-and-Research/Publications-and-media/NFPA-Journal/2021/Spring-2021/Features/Cybersecurity

utility infrastructure. Manufacturers of these systems need to be more aware than ever of system vulnerabilities, making organizations aware of when they might be exposed and patching the problem as expediently as possible. Organizations devoted to fire safety need to do more to publish codes and standards for fire protection systems. The National Fire Protection Association (NFPA) is making strides to not only increase awareness but to start an industry standard of best practices and responsibility with the release of their research document titled, Cybersecurity for Fire Protection Systems.[2] When all is said and done it may not be possible to be 100% protected against cyberthreats but organizations can certainly do their utmost to make themselves seen as “more trouble than they are worth” or by reducing the damage as much as possible.

[2] https://www.nfpa.org/-/media/Files/News-and-Research/Fire-statistics-and-reports/Building-and-life-safety/RFCybersecurity.pdf

While Intact Public Entities Inc. does its best to provide useful general information and guidance on matters of interest to its clients, statutes, regulations and the common law continually change and evolve, vary from jurisdiction to jurisdiction, and are subject to differing interpretations and opinions. The information provided by Intact Public Entities Inc. is not intended to replace legal or other professional advice or services. The information provided by Intact Public Entities Inc. herein is provided “as is” and without any warranty, either express or implied, as to its fitness, quality, accuracy, applicability or timeliness. Before taking any action, consult an appropriate professional and satisfy yourself about the fitness, accuracy, applicability or timeliness of any information or opinions contained herein. Intact Public Entities Inc. assumes no liability whatsoever for any errors or omissions associated with the information provided herein and furthermore assumes no liability for any decision or action taken in reliance on the information contained in these materials or for any damages, losses, costs or expenses in a way connected to it. Intact Public Entities Inc. is operated by a wholly owned subsidiary of Intact Financial Corporation.