Last month I, along with 40,000 other people, attended the annual RSA Conference in San Francisco. Between the sales pitches, the seemingly acres of trade show booths and wall-to-wall people, there were some great speakers talking about what to expect in cybersecurity in the future.

Ransomware is a very big subject in 2017. My post “I’ll Take Ransomware for $17,000” spoke about this in depth.   A lot of companies are being proactive to deter the chance of ransomware. Is yours?

The Internet of Things (IoT) and the Industrial Internet of Things (IIoT) also gained a lot of attention at this conference. While the interdependency of various parts of one’s facility has existed for years, there is the technology that now allows one the convenience of being able the HVAC system to the alarm management system from a remote location. And in some cases, from one’s smartphone! While the convenience is welcome and can lower costs and boost productivity, one must be fully aware that the IIoT can expose vulnerabilities in your system and provide a pathway for hackers to get into other systems.   Did you know that the Target breach came through the operating system for their HVAC?

But the topic I heard most, both in presentations and on the trade show floor, is an insider threat. The term “insider threat” conjures up images of some radical on your staff who has been trained to bring down your IT or industrial control system when given the orders from the syndicate, cell, or whatever. While that is a possibility, the more likely event is a well-meaning employee doing something stupid. This could be leaving a password written on a sticky note next to the computer or charging their phone by plugging it into the USB drive on the network. But, most likely, they click on a link in a phishing email.

The insider threat can be mitigated by good background checks and education. Many companies offer software that can simulate a phishing email and let you know who clicks it. This is a great educational tool, as it will allow you to see who is vulnerable and you can teach them what to watch out for in emails. A well-meaning employee will only need to be told once.

There are other things such as artificial intelligence, cryptology, and robotics that are becoming bigger issues in cybersecurity. The landscape is constantly evolving. The AFPM Cybersecurity Subcommittee keeps on top of these changes so AFPM members can be proactive in the cyber defense of their facilities.

Print as PDF:

Topics

Security

Cybersecurity

Tags

Cybersecurity

Insider Threat

AFPM Cybersecurity Subcommittee