Mike Galler

Basic Recommendations For HVAC Cybersecurity

BY MIKE GALLER, MEMBER ASHRAE

Cybersecurity has been a topic of increasing importance for several years. While fully securing a large, complex system can be complicated, some basic precautions can easily be applied to any system. This column provides introductory information on recommended cybersecurity precautions for HVAC networks that would be helpful to facility staff with limited expertise in cybersecurity.

There have been many headlines about major cybersecurity breaches at large companies, but administrators of small networks also need to be concerned. Malware does not care about the size of the company owning the computer or the network it is attacking. Failing to address the needs of cybersecurity is like failing to prepare for a hurricane because you think you're too small for the hurricane to care about. Recent statistics show that small businesses are frequently the target of cyberattacks.[1–7]

A good cybersecurity plan addresses the physical components of the facility and the personnel, policies, legal, liability and education requirements. No "one-size-fits-all" exists when it comes to protecting a facility from attacks. Knowing your levels of risk[8] and cybersecurity awareness, likely threat vectors, technical abilities and your budget will help create a workable plan.

Many recommendations for securing industrial control systems outlined in NIST SP 800-82[9] are relevant to building automation systems. These include access control, identification and authentication, configuration management, awareness and training and planning. Multiple controls are suggested for each of these areas, providing a range of recommendations and guidance. Cybersecurity relies on defense-in-depth; implementing more precautions will make your network safer. This column will briefly explore two of these areas: awareness and training and planning. Future columns will address the remaining areas: current issues in cybersecurity and advances in technology relating to cybersecurity.

Awareness and Training

- Every person who will use a computer on any network operated by their business must be aware of basic cybersecurity concepts. Your HVAC equipment on the operational technology (OT) network may be protected by a virtual private network (VPN), but it will still not be secure if your information technology (IT) network is compromised. Many types of malware are spread through fraudulent e-mail designed to look legitimate. Malware may also be disguised as a different program offered for download. Training employees to recognize

Mike Galler is an engineer at the National Institute of Standards and Technology in Gaithersburg, Md. He is the chair of ASHRAE's Cybersecurity for HVAC Systems and Related Infrastructure Multidisciplinary Task Group.

malware is an important part of the strategy to defend your network. Free and low-cost online cybersecurity training is available.[10] Be sure to select training that is matched to the employee's roles. A budget should be allocated for employees who have roles that require specialized training.

- Define your cybersecurity policies for your human resources department, operations and maintenance department and contractors. Make sure a compliance verification process exists for these policies. Policies must be followed accurately to be effective.
- Cybersecurity attacks evolve over time. Your training and policies must also evolve to meet new threats.

Planning

- Cybersecurity planning must encompass the entire life cycle of the building and the systems and networks that support it. Guidance on developing a security plan can be found in NIST SP 800-53.[11]
- The network configuration must be designed around the concepts of cybersecurity. Trying to retrofit cybersecurity onto the network later may require more effort with less effect.
- Develop a comprehensive design and implementation plan regarding your building control system. Engage your consulting engineer, IT and IT security team, IT security auditor and OT team in proper sizing and scope of cybersecurity measures. Do this *before* it becomes an issue, not after the breach has occurred.
- Engage with your legal advisers on creating and enforcing cybersecurity insurance, contracts, indemnification and related policies. They can also develop legal documents relevant to contractors working on building systems.
- If a breach does occur, have a notification, triage and escalation plan in place to reduce any negative outcomes.
- As with other building components, cybersecurity will require a level of ongoing maintenance to ensure adequate security controls continue to be implemented as intended. It is important to plan for this when allocating resources.
- All computers and network components should be in environmentally controlled locations. A computer is less likely to fail if it is kept clean and up-to-date. Dirt, dust or other debris can clog fans or heat exchangers in the computer and cause components to overheat. Operating system updates should be installed after they are approved by the HVAC systems vendor.
- If your computer has a conventional hard disk drive (HDD), industry recommendations are for it to be replaced after three to five years due to the probabilistic nature of HDD failures. It is recommended to replace it with a solid-state drive (SSD) due to their generally higher durability and reliability.

Conclusion

This list is intended to be a basic introduction to cybersecurity. A deeper understanding of relevant topics is necessary to ensure your network is secure. For more information about cybersecurity, see the *2019 ASHRAE Handbook—HVAC Applications,* Chapter 41, Computer Applications, Section 5. In addition, ASHRAE Guideline 13-2015, *Specifying Building Automation Systems*, has a new chapter specifically addressing cybersecurity requirements. Multiple sources of information are also available on the internet, including more detailed recommendations and references to applicable standards.

References

1. Palmer, D. 2019. "Two Cybersecurity Myths You Need to Forget Right Now, If You Want to Stop the Hackers." ZDNet. https://tinyurl.com/p558xjbn

2. Crane, C. 2020. "15 Small Business Cyber Security Statistics That You Need to Know." The SSL Store. https://tinyurl.com/v5dzx5yh

3. Paulsen C., P. Toth. 2016. "NISTIR 7621, Rev. 1—Small Business Information Security: The Fundamentals." National Institute of Standards and Technology.

4. FBI. 2021. "2020 Internet Crime Report." Federal Bureau of Investigation. https://tinyurl.com/k65kev7k

5. Steinberg, S. 2019. "Cyberattacks Now Cost Companies $200,000 on Average, Putting Many Out of Business." CNBC.com. https://tinyurl.com/jykp3s26

6. Sobers, R. 2021. "134 Cybersecurity Statistics and Trends for 2021." Varonis.com. https://tinyurl.com/2hc672fy

7. Walker, I. 2019. "Cybercriminals Have Your Business In Their Crosshairs, and Your Employees are In Cahoots With Them." Forbes.com. https://tinyurl.com/4p79m3ds

8. NIST. 2012. "SP 800-30, Revision 1—Guide for Conducting Risk Assessments. National Institute of Standards and Technology.

9. Stouffer, K, et al. 2015. "SP 800-82, Rev. 2—Guide to Industrial Control Systems (ICS) Security." National Institute of Standards and Technology.

10. NIST. 2020. "Free and Low Cost Online Cybersecurity Learning Content." National Institute of Standards and Technology. https://tinyurl.com/2tmz6jtu

11. NIST. 2020. "SP 800-53, Rev. 5.—Security and Privacy Controls for Information Systems and Organizations." National Institute of Standards and Technology. ■