BILL BOOTHE
Bill Boothe is president and owner of The Boothe Group, LLC, an independent consulting firm that helps clubs understand computer technology, make good decisions and receive the highest value from their technology investment. Bill can be reached at bboothe@boothegroup.com.

Cybersecurity: A Guide for You to Follow

Every once in a while, we get lucky and someone produces a report or white paper that offers valuable advice for the private club industry. Voila!

Just such a document was published last year as a collaboration by Hospitality Financial and Technology Professionals (HFTP) and the National Club Association (NCA). It's named "Comprehensive Practices in Club Cybersecurity." Yet somehow, this gem has flown under the club industry radar as few club managers seem to be aware of its existence.

For most readers, the problems with research reports and white papers are: too long, too detailed, too technical. "Why can't they just get to the point and tell us what we need to do?" OK, here's the "Cliffs Notes" version of this 35-page report.

First off, after you skip past the Table of Contents, the bios of the Advisory Committee and Contributing Authors, the Forward and the Introduction, you're already on Page 7; another five pages cover Risk Terminology and Governmental Regulations; and eight more pages at the end of the report cover Reporting and a Case Study. So, the What You Need To Do part of the report is only 16 pages. While the Best Practices section covers a wide range of cybersecurity topics, below are, in my opinion, the top three for you to focus on initially.

Employee security awareness training (SAT). SAT is a formal process for educating employees about ever-evolving cyber threats and their role in protecting the organization. Online security awareness training arms employees with tools and training that help them avoid cyberattacks aimed at computer users. Since a high percentage of breaches are inadvertently "assisted" from within the organization, it makes sense to train our employees to recognize and avoid the most common ploys (most likely phishing emails).

SAT is best provided through a formal program from an outside company. The program includes ongoing training and awareness sessions along with regular "testing" of employee awareness.

Secure remote access. When employees connect to the club's computer network from a remote location, two terms should resonate here: virtual private network (VPN) and cell phone hot spot. A VPN is an encrypted "tunnel" between the remote PC and the club's network. It hides your transmission from outside intruders. As the quote explains, "If an attacker can't see it, they can't hack it."

Hackers often create fake public Wi-Fi sites that redirect the remote user to their networks. The hacker then loads malware onto the user's PC. Employees can easily avoid using public internet networks (at hotels, airports, restaurants, etc.) that could be compromised. Instead, they should use their cell phone's hot spot feature. A hot spot creates a personal Wi-Fi connection for private access to the internet that outside intruders cannot access.

Intrusion detection. Think of this technology in terms of your home's alarm system. While you have locks on the doors and windows, the alarm system activates when an intruder has broken through the locks and is entering your home. The computer equivalent of a home alarm system is called intrusion detection. In its most basic form, intrusion detection is provided using a technology called file integrity monitoring (FIM). It's actually software that scans the operating system (Windows), application software and databases to determine if they have been improperly changed or corrupted. If it detects any corruption, an alarm is issued. Plus, FIM will shut down the suspected rogue user's access to the network and/or will temporarily shut down the whole network as a safety precaution.

An advanced form of FIM is called unified threat management (UTM). This is a physical appliance that maintains multiple security layers, all within a single device. Most clubs protect their network with a variety of products from different manufacturers: anti-spam, anti-malware, intrusion detection, and network firewalling. But these days hackers are using "blended threats" that combine several methods that attack multiple areas of the network simultaneously. UTM is better able to detect and handle these complex threats than separate security tools.

The bottom line: To be safe, you should follow every bit of advice offered in the HFTP/NCA "Comprehensive Practices in Club Cybersecurity" document. But let's get serious. Rarely does anyone do everything they should do. However, deploying just these few technologies – SAT, VPN, cell phone hot spot, and intrusion detection – will provide your club with a very high degree of cybersecurity. Don't wait. The bad guys are at it full time – and clubs are in their sights. BR