Cyber Security
THE REAL STORY

BILL BOOTHE

JEFF HALL

There's a lot of buzz in the club industry these days about cyber security. As a result, many clubs are buying cyber security services to shore up their "protected data." Trouble is, much of the hype by the service providers is at best confusing if not a bit misleading. Here's the real story.

Clubs are required by state laws to secure their "protected data." That would be member and employee data stored on the club's computer systems. Each state's laws are different, but essentially they require companies to protect any data that could be used by an outside bad guy to steal the person's money or identity.

So social security and driver's license numbers, credit card and bank account information, along with demographic information such as names, addresses, phone numbers, email addresses, spouse names, children's names, universities attended, professions, home states, and photos – essentially any data point that could connect a bad guy to the member – must be protected.

For many years private clubs took an "it can't happen here" attitude toward serious cyber security. But of late the industry has recognized that the threats are real, and the damage that can be done to members – and ultimately to the clubs themselves – is substantial. So clubs are beginning to embrace cyber security services. Typically, the services fall into one of two categories:

1. Network intrusion security review: This service generally begins by attaching a scanning device and/or scanning software to the club's computer network to determine if there are intrusion risks to the systems. Initial scans focus on the ability of the network firewall(s) to repel *external* attacks. The scanning continues by evaluating the ability of the systems to thwart intruder activities if the hacker is able to get past the firewall and gain access to the network.

This *internal* risk evaluation focuses on missing security patches, password strength and password changing rules, the presence of discontinued or unsupported software such as Windows XP, the absence of web filtering (controlling what Internet sites employees are allowed to access), adequacy of anti-virus and anti-malware solutions, etc. The point of the review is to identify any weaknesses that may allow an outside intruder to gain access to the club's network – or once inside, may allow that intruder easy access to protected data.

2. Social engineering testing: Because most businesses have very strong external protection with an effective firewall, bad guys have changed tactics. Why try to fight through a strong firewall when you can easily go around it?

Now that social engineering has become the favorite attack method of outside intruders, less than 20 percent of all small business intrusions are perpetrated without the "help" of an insider. The other 80 percent are the direct result of employees inadvertently "assisting" the bad guys by taking the social engineering bait. Unfortunately, this gaping hole in club security is essentially ignored by the vast majority of "cyber security" service offerings.

Social engineering does just that by using various ploys to trick the club's employees into inadvertently allowing access to an outside intruder. The ploys include sophisticated phishing emails, telephone calls and in-person visits by impersonators and other actions

intended to dupe employees into providing network access information. Social engineering testing is designed to identify the likelihood that *employees would inadvertently assist* an outside intruder to gain access to the club's network – and as a result, acquire protected data.

Thus far the club industry seems to be firmly focused on network intrusion security reviews. A litany of companies, some local, some national, are peppering clubs with promotional information about the dangers of not having their networks secure and intrusion-proof.

All well and good, but here's the rub. Now that social engineering has become the favorite attack method of outside intruders, less than 20 percent of all small business intrusions are perpetrated without the "help" of an insider. The other 80 percent are the direct result of employees inadvertently "assisting" the bad guys by taking the social engineering bait.

Unfortunately, this gaping hole in club security is essentially ignored by the vast majority of "cyber security" service offerings. You'll have to look a bit to find companies that go beyond physical security to focus on social engineering testing.

In addition, as a preventive measure, training is available from several national sources that will teach employees how to recognize and avoid social engineering ploys. Completing that training can not only help secure the club's protected data, but it can also reduce the club's cyber security insurance premiums and help mitigate damages in the event the club experiences a breach of protected data.

To cover all the cyber security bases we recommend the following:

- Have a reputable company conduct a network intrusion security review.
- Have a different reputable company conduct the social engineering testing.
- Have a third reputable company provide training to your club's employees on how to avoid taking the social engineering bait. **BR**

Bill Boothe is president 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. During his 25 years in the club industry Bill has assisted more than 350 private clubs. Bill can be reached at bboothe@boothegroup.com.

Jeff Hall is a principal security consultant with Optiv Security, Inc., a cyber security consulting firm. Since 2003, Jeff has been focused on securing sensitive authentication data related to card transactions following the Visa, MasterCard, and PCI Security Standards Council standards. Jeff can be reached at jeff.hall@optiv.com.