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. During his 28 years in the club industry Bill has assisted more than 400 private clubs. Bill can be reached at bboothe@boothegroup.com.

Why Private Clubs Are Targets for Cyber Attacks

Because that's where the money is! – Attributed to Willie Sutton, when asked why he robbed banks in the 1920s, although he subsequently denied making the statement.

It should be obvious to private clubs why they are prime targets for cyber attacks. But somehow the club industry continues to go along its merry way with little regard for the serious peril awaiting just around the corner. Some facts that help support the need for industry-wide concern include:

- Private clubs are small businesses
- 43 percent of cyber attacks are on small businesses
- Many members of private clubs are affluent individuals
- Private clubs maintain Personally Identifiable Information (PII) on their members
- PII of affluent individuals is highly-prized by hackers
- PII is used by hackers to develop identity theft profiles
- Stolen identities are used to open fraudulent bank and credit card accounts, take out fraudulent loans and mortgages, etc.

So, clubs *fit the mold* as excellent targets for cyber attacks intending to gather PII. Is the typical club adequately protected? In my experience, not even close. Here's why.

Network security – The first layer of protection. Most clubs have adequate firewalls, passwords, etc. to ward off a frontal attack from an outside intruder. Unfortunately, hackers know this and generally focus their efforts on other attack modes. In other words, since the front door is well protected, they focus on the back door for entry.

Phishing (generic) and spear phishing (personalized) emails – An easy back door way for hackers to get around network security. These emails are authentic looking and effective in enticing unwary club employees into opening the back door.

- 52 percent of data security breaches are inadvertently assisted by employees of the business.

No alarm system – Even if a hacker successfully invades a club's network, standard monitoring methods are available to quickly identify intruder activity and choke it off. Sadly, very few clubs use such monitoring. This allows intruders to explore the network at their leisure, looking for valuable PII.

No employee awareness training – Lots of companies offer training designed to teach staff how to identify and avoid phishing emails. Sadly, very few clubs (or other small businesses) utilize such training. No wonder that more than half of all system breaches are assisted by unwary employees.

How real is the threat? During the past two years I've been asking club financial executives attending my education sessions to fess up about the level of attacks they are experiencing. A disturbing 25 percent acknowledge that their networks have been compromised during that period.

Almost all have been ransomware attacks where (thankfully) the club has regained control of its systems by paying a ransom (sometimes as high as $10,000). But what's even more troubling about those attacks is that very few of the clubs have any idea if member PII was copied/stolen while the hackers were in their systems.

Bottom line – It's wide for clubs to deploy employee awareness training to secure the back door and network monitoring to quickly choke off any intruder who manages to invade the network. BR