Cyber Attacks Put Directors and Officers at Risk

ROB MULHERN

The hacking of retail giant Target Corp. last holiday season resulted in the theft of 40 million credit and debit card records, along with 70 million other records including addresses, phone numbers and additional customer information.

And identity theft affects organizations of all sizes and in many different industries.

Golf and country clubs and other private clubs are no exception. In fact, with the volume of credit card swipes at their bars, restaurants and pro shops, clubs offer ample opportunities for cyber attacks. Plus, stored on computers are member and prospective member applications and files with social security numbers, driver's license numbers, dates of birth and credit card numbers, along with employee and vendor data.

Cyber attacks can result from simple employee mistakes, such as loss of a laptop containing club accounts, or they can be part of intentional acts of theft by employees or outsiders. For example, food and beverage servers may swipe customer credit cards in pocket size devices over an extended period of time and then sell the data.

The fallout from these cyber attacks can diminish the trust members have in a club, affecting both your bottom line and reputation. But these attacks also carry personal risk for each board member and officer, according to Brian Thornton, president of ProWriters, a specialized provider of professional and management liability insurance.

"With heightened regulation and an increased focus on corporate governance, it's important for directors and officers to focus on cyber and privacy risk management," Thornton says. "Robust insurance coverage is available for golf clubs including coverage for first party costs, third party liability, pre-breach risk management services and post-breach services to help manage an incident as it unfolds."

According to Thornton, while the cost of cyber liability coverage was initially high, more insurance carriers have entered the market, creating increased competition and driving down premiums to more affordable levels. These policies cover the costs of notifying affected members, prospective members and any others whose data may have been hacked. They also cover public relations costs to minimize harm to your club's reputation and the potentially expensive computer forensic costs to unravel how you were hacked and by whom.

Other coverage typically included in these policies are cyber business interruption, legal defense costs, government fines and remediation, cyber extortion and multimedia liability.

Insurance policies like this often make available risk management services that can prevent cyber attacks from happening in the first place. Since many clubs do not have full IT departments, the use of outside consultants can be a valuable tool to help build necessary firewalls, data encryption and other safeguards. You need to know how your data is vulnerable and what safeguards are applied to each computer and device. You also should see a network map that shows where data is stored and who controls it.

Along with technical protections, there are questions you should ask about board governance and information management: Who is in charge of cyber security at your club? What is the role of board oversight in ensuring necessary steps are taken to protect club data and member privacy? Where are you most vulnerable to a cyber attack? Do you have cyber security built into your club's emergency response plan so you can respond quickly and appropriately?

Club board members and officers are valuable positions that bring many benefits, but they also are laden with personal risk. When looking at your D&O coverage, boards should take a proactive approach that includes embracing cyber liability risk management and insurance coverage. **BR**

Rob Mulhern is senior vice president of PREFERRED CLUB (www.preferredclub.com), an industry-leading insurance program for golf and country clubs nationwide. He can be reached at rmulhern@ventureprograms.com.