The New Crime Wave

Social Engineering, Employee Dishonesty, and Cyberattacks at the Golf Course

VGM Insurance & Financial Solutions

800.362.3363 | info@vgminsurance.com

Protecting Your Intangible Assets

Imagine a couple of men walk into your country club with badges, walkie-talkies, and proper identification. They tell the receptionist at the front desk they are performing a routine sprinkler inspection. Your receptionist lets them in because they look and play the part perfectly. The two men split up, seemingly conducting different parts of the inspection, and return to the receptionist 15 minutes later, explaining they have completed their assessment. They walk out the door and are never seen again. Nothing to worry about, right?

Wrong. You've just been the victim of a well-thought-out social engineering fraud (SEF) scam. Days or weeks later, your computer system is compromised, customer credit card numbers are stolen, and sales are dropping. So, what happened?

What Is Social Engineering Fraud?

SEF happens when attackers take advantage of human behavior to commit a crime. Social engineers can gain access to buildings, computer systems, and data simply by exploiting the weakest link in a security system—humans. Golf courses and country clubs are especially vulnerable to these scams due to the nature of the business and the frequent inspections by third parties needed to remain in compliance (think pool inspections, fire safety, sprinkler systems, liquor licenses, junior programs, food safety inspections, and so on).

Social Engineering Tactics

If you can learn to identify the ways in which a social engineer might try to break into your business, you can stop a threat before it begins.

Social engineers are masters at blending in. They research their target for weeks or even months, learning the smallest details to gain entry into a company. They are often sweet-talkers and their body posture lets others believe they belong.

Social engineers often work in groups of two. In the opening example, the two men split up to conduct a "sprinkler inspection." Keeping them together could have saved the company a lot of time and money. Always make sure there are eyes on visitors at all times.

Employee Dishonesty

It's not only third parties that are capable of using social engineering tactics to commit fraud against an organization. There are many cases where employees at golf courses and country clubs have taken advantage of member generosity to steal from a club. Here's one example:

A controller at a club sends a message to club members letting them know about a large expansion project for the clubhouse—a new pool, fitness facility, yoga studio, and restaurant upgrades. They ask club members to wire money to a specific account to pay for the project (which is a standard procedure at a club for capital projects like this). However, the wire transfer reroutes a portion of the money directly to the controller before landing in the club's account. The controller does this for many years before being caught.

Can this really happen? Yes. Just last year the chief financial officer at a club in Texas, an exclusive private residential community known for its famous guests, was fired after board members found the CFO had been falsifying documents for 12 years. The former CFO allegedly falsified documents to mislead general managers and boards of directors into thinking the club had no debt. Officials found the company owed $5.2 million.

How to Prevent Social Engineering Fraud

Being the victim of a social engineering scam can have a wide range of effects on your business, including:

- Damaged reputation
- Lost sales
- Humiliation
- Lower staff morale
- Losing customer base

All these effects take a lot of time and money to reverse. Because humans are naturally trusting, it can be difficult to identify when we are being socially engineered. However, there are ways to prevent social engineering from potentially ruining your business:

- There should be policies in place at your business that limit or eliminate the amount of sensitive information that is made available to your employees, customers, or the general public. Never allow employees to give out passwords or credit card numbers over the phone. If this information is needed by another employee, meet face-to-face.
- Make sure employees never write down their passwords on paper. A piece of paper with important passwords on it can be swiped by a social engineer in the blink of an eye. Make sure your employees' computer passwords expire after a set amount of time, generally three months. Set guidelines for new password creation, but keep in mind that complex passwords are difficult to remember. If passwords are reset too frequently or are too hard to remember, employees will end up creating passwords that can easily be guessed.
- Consider installing security cameras around your building. Make sure to keep an eye on areas where security is lax, such as a smoking area or near an unguarded back door.
- All visitors should be greeted and presented a sign-in sheet to fill out.
- Prohibit employees from posting work-related information on social media websites. Often, social engineers spend weeks or even months learning about employees' habits and tendencies before making a move. A simple post about being out of the office for a short length of time could be all a social engineer needs to steal sensitive information. Let employees know that posting otherwise harmless information on the internet, such as a telephone number or address, could be the final piece of a social engineer's plan of attack.
- Have employees wear badges with their name and picture on them, and have employees swipe their badge to gain access to different areas of the building. Let your employees know that it is not OK to let in employees they don't recognize because they "forgot their badge." This is a common technique to get social engineers in the building.
- Subject your company to penetration testing. Hire an outside agency to act as a social engineer and see how your employees respond. If the test is successful, your employees will be embarrassed. That can lead to extra motivation to be vigilant of social engineers if they were to try to gain access to your company.

Which Insurance Policy Will Protect My Business

It can be confusing which insurance policy should cover these kinds of losses. Crime policies cover the misuse of funds, employee dishonesty, embezzlement, extortion, forgery, and computer fraud, while Cyber policies cover losses that result from unauthorized data breaches or system failures. Often, these policies are covered by different carriers, too, which results in even more complication when a claim arises.

Our best advice is to get your insurance broker and legal team together today to discuss possible claims scenarios involving social engineering, employee dishonesty, and cyberattacks. Ensure you have the correct coverage in place, and have a response and remediation plan at the ready. While social engineering fraud and claims of this nature are still very much a gray area, they are on the rise, and the best thing your club can do is be prepared.

For more information, reach out to our golf insurance experts at ***info@vgminsurance.com*** or ***800-362-3363***.

Insurance & Financial SOLUTIONS