LINDABURY

McCormick, Estabrook & Cooper, P.C.

Attorneys at Law

Protecting Your Business From Social Engineering Attacks

Countless ways into your company's IT system exist. Proactive management of vulnerabilities can mitigate opportunities for social engineering

Cybersecurity & Data Privacy

Recognizing & Avoiding Social Engineering Attacks

What is Social Engineering?

Social engineering is a broad term to describe the practice of using social interactions and deception to obtain or compromise financial or computer information. It can be a cheap, easy and low tech way for hackers and cyber criminals to gain access to a company's protected information. In fact, the majority of existing malware is designed to trick a user through some type of social engineering scheme rather than exploit a technical flaw in a system or program. This is a wise strategy for hackers since it is estimated that computer users account for more than 90% of cybersecurity incidents.

- The social engineer targets companies and individuals by posing as a legitimate contact such as a client, employee, creditor or vendor in order to further the deception and gain access to company information.
- Social engineers also target people's natural curiosity by sending e-mails or social media posts containing intriguing or attention-grabbing headlines and files or articles embedded with malicious links or software.
- Social engineering comes in many forms:
  - It can involve direct communication such as phone scams or physical interaction such as "shoulder surfing" or "tailgating" (e.g., a fake delivery person following an employee into a secure area).
  - Social engineers can also monitor social media and other sources to secure personal information to be used in a broader, more significant cyber-attack.
  - Phishing involves sending e-mail or social media messages to trick a person into providing personal information or to infect a computer system with malware or ransomware. Hackers often pose as a trustworthy or recognized entity, business associate or co-worker. More sophisticated hackers use e-mail or websites which appear legitimate and may include detailed business or personal information which makes an attack more difficult to detect.

The Cost of Social Engineering

The business cost of social engineering and cyber-attacks is eye opening. A study conducted in 2015 estimated that the cost for an average company to contain malware is $1.9 million. Another study estimated that the average organizational cost of a data breach is $7.01 million. The total cost of cyber-attacks on global business was estimated to exceed $300 billion last year.

Potential costs to companies include:

- expenses for investigation, regulatory compliance, legal and public relations and lost business/revenue
- A company may also be responsible for costs associated with customer notification and protection and potential fines and penalties for regulatory violations in the case of the theft of customer financial data
- Long term costs for a company could include increased insurance premiums and the loss of a company's reputation and good will

These risks apply to companies of all sizes. IBM recently estimated that small and mid-sized businesses account for 60% of all cyberattacks. Such companies, which are generally less sophisticated and less prepared to deal with cyber-attacks, may make more attractive targets to hackers and cyber criminals.

Managing The Risk of Social Engineering

Companies can take certain steps to help mitigate the risk of social engineering. Some of the general steps are as follows:

- Establish and maintain an effective cybersecurity program with clear rules/procedures.
- Constantly update and monitor computer systems and network.
- Educate and train employees and management on how to identify, avoid and respond to social engineering and cyber-attacks.
- Create a phishing incident and data breach response plan and rehearse responses to various attacks ("fire drills").
- Consider purchasing cyber liability insurance to cover the potential costs associated with a socially engineered cyber-attack.
- Consider retaining an expert to evaluate and test network security. and evaluate a company's policies and ability to prevent and respond to social engineering and cyber-attacks.

Despite the potential dangers and costs of social engineering, companies can help protect their financial and customer information by educating themselves and taking a proactive approach to cyber security.

For Specific Questions Concerning Your Company's Cybersecurity, Please Visit lindabury.com or Call 908.233.6800 to Speak to Any of Our Cybersecurity & Data Privacy Attorneys