EPIC Insurance Brokers & Consultants

CYBERSECURITY

SOCIAL ENGINEERING FRAUD

WHAT IS SOCIAL ENGINEERING FRAUD?

Social engineering most commonly occurs when hackers manipulate employees into voluntarily parting with company or client funds money or products. Hackers take advantage of human nature to exploit a target company through its employees. Social Engineering usually involves an email or other type of communication that induces a sense of urgency in the victim, which leads the victim to promptly comply. By educating staff to be alert to these tactics, companies can reduce the risk of falling prey to such schemes.

SOCIAL ENGINEERING FRAUD TECHNIQUES

- **Pretexting:** Hacker impersonates someone in authority in an effort to obtain personal information or some sort of action.
- **Phishing:** Use of phone or internet to "phish" for data that could be used for pretexting, sending malware, or to obtain information.
- **IVR Phone Phishing:** Uses voice response system designed to impersonate a bank or other financial institution.
- **Quid Pro Quo:** Bribery or blackmail in return for the release of confidential information.

REDUCING THE RISK OF A SOCIAL ENGINEERING FRAUD LOSS

- Establish procedures for transferring any money by wire.
- Establish a verification system involving communication over multiple mediums to ensure legitimacy of financial transactions.
- Avoid offers that sound too good to be true, because they most likely are, especially those offered by email.
- Implement training programs that build corporate awareness and teach employees how to detect some of the psychological tricks (such as power, authority, and pressure) used by cybercriminals.

DON'T BE A STATISTIC

A cyber attack takes place every **39 seconds**[1]

43% of hackers target small businesses[1]

Over 75% of the healthcare sector was infected by malware in 2018[1]

CLAIM EXAMPLE

An employee received emails supposedly sent by the CEO and the company's audit firm. The emails instructed the target to wire millions to a Chinese bank. The first emails insisted on absolute secrecy, citing the confidential nature of the "transaction", and directed that all communication be through email. A later email instructed the target to contact an employee of the company's accounting firm for details on where to transfer the money. The phone number and contact were fraudulent and set up specifically to dupe the victim.

What made it work? The emails looked like they were legitimate, and there had been ongoing rumors that the company had expansion plans in China. The good nature and trust of the employee coupled with a lack of adequate verification procedures led to a loss of **$17.2 million.**

[1]Cybint's "15 Alarming Cyber Security Facts and Stats article: https://www.cybintsolutions.com/cyber-security-facts-stats/

EPIC Insurance Brokers & Consultants

CYBERSECURITY

SOCIAL ENGINEERING FRAUD

INSURANCE SOLUTIONS FOR SOCIAL ENGINEERING FRAUD

CYBER COVERAGE

Cyber risk mitigation involves taking proactive steps to protect against and reduce the adverse effects of the key risks to your organization. Implementing network security defenses, incident response plans and employee training are all essential elements of cyber risk mitigation. Unfortunately, this is not enough. The reality is, no organization is immune from a cyber-attack, regardless of the strength of their defenses. This is where insurance can help. Comprehensive stand-alone cyber insurance will help protect the organization's balance sheet by transferring some of the costs associated with the inevitable breach.

Cyber insurance complements and supports active security measures by providing third-party regulatory and liability coverage as well as a host of first-party response, remediation and recovery insurance. In addition, most cyber markets also provide free or discounted pre-loss services to assist an organization in breach preparedness.

RISK MANAGEMENT TIPS

- Develop, implement and regularly update and test a holistic incident response plan that includes IT, HR, Accounting Staff, Security and Management
- Appoint a Computer Information Security Officer
- Identify, contain and protect any Personal and Corporate Confidential or Sensitive Information.
- Continually maintain and upgrade computer systems and software
- Implement mandatory employee training to better prevent phishing, unauthorized transfer of funds, or unwitting data breach
- Encrypt all mobile devices

CRIME COVERAGE

Commercial Crime insurance provides first-party coverage intended to help an organization recoup losses due to employee dishonesty, theft of money or securities, robbery, burglary, forgery and alteration, and theft of client property. In addition, Commercial Crime policies also typically include coverage for Computer Fraud, Wire Transfer Fraud and Social Engineering Fraud. Today, many stand-alone cyber policies also include similar or identical coverage extensions. This means there is a potential for overlapping and/or redundant coverage. Organizations should strive to coordinate coverage between stand-alone cyber and crime policies in order to ensure they are able to maximize potential insurance recoveries in the event of an incident.

In addition to the above, most commercial crime policies also provide a limit for investigation costs for covered loss, assisting the insured in paying for the complex process of determining the extent of the loss once the fraud has been uncovered. Coverage is typically on a loss discovered basis, meaning that the cumulative loss over time, regardless of when it took place, is covered by the policy in place when the loss is discovered.

RISK MANAGEMENT TIPS

- Establish an anti-fraud policy and code of conduct, with a hotline for employees to call if they suspect fraudulent activity. Conduct anti-fraud training and procedures for employees, managers and executives
- Conducting external audits of internal controls used in financial reporting
- Maintain multi-person controls in accounting and inventory
- Vet, update and purge approved vendor lists at least annually