CRAIN'S CUSTOM MEDIA
A DIVISION OF CRAIN'S CHICAGO BUSINESS

Are You Covered for Social Engineering Fraud?

An interview with **ANGELA ELBERT,** chair of the Insurance Policyholder Practice Group at Neal Gerber Eisenberg, Chicago.

What types of insurance claims should most concern today's senior executives?

Social engineering fraud is a growing threat that involves criminals deceiving victims to give away funds. For example, an employee might follow instructions from a high-level officer or other presumably authorized employee to transfer funds to an account supposedly held by a vendor. Ultimately the officer or authorizing employee may not be legitimate, or the supposed vendor account may actually be controlled by the fraud's perpetrator. These scams can be initiated in person, over the phone, or via email or social media. They're unsettling because the techniques employed by the scammers have become sophisticated, professional and believable.

How serious is the threat? What's at stake?

An October 2018 report by the SEC estimated nearly $100 million in unrecoverable losses from social engineering frauds for just nine undisclosed companies. It also reported FBI estimates of $5.7 billion in overall losses in this category since 2013—the highest amount of loss for any class of cybercrime during that period.

How should companies prepare for this threat? What sort of insurance is available?

Executives frequently have the misconception that their existing insurance—often cyber insurance—covers social engineering fraud. Some cyber insurance, however, only covers losses from data breaches, not from social engineering fraud. Cyber policies may also be limited to losses perpetrated through email or hacking, as opposed to phone or fax. Similarly, commercial crime policies may limit what risks are covered, and may not include coverage for all of the types of social engineering fraud that criminals increasingly employ.

The best thing a company can do is educate its employees on how to spot a scam. The recent SEC report emphasized the importance of companies revising procedures and implementing stronger internal accounting controls as a way to prevent social engineering fraud.

A company can mitigate the financial risks of falling victim to a scam by purchasing a social engineering fraud endorsement on either its existing cyber insurance or commercial crime policy. Many companies aren't yet aware that these endorsements exist. When a company applies for this type of coverage, in order to qualify, insurers take a close look at the company's internal control procedures and verify that they closely track the requirements of the endorsement. This process also helps businesses prepare for potential threats.

If a company handles money for clients, and especially if it sends payments to vendors, it should consider purchasing a new form of endorsement that may be available to cover a situation in which a representative of the insured is duped into giving away a client's funds, rather than funds of the insured entity.

How should companies assess the coverage they'll need to address this particular threat?

Many businesses aren't aware that they can seek higher sublimits—the maximum amount available to pay for that type of loss—than those initially offered by insurers. We advise them to obtain the greatest limits possible and determine if any excess coverage will allow additional sublimits for social engineering claims.

NEAL
GERBER
EISENBERG

Contact: aelbert@nge.com • 312-269-5885