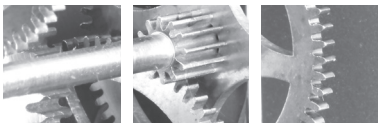
Aon Advisor Solutions

Fall 2018 Newsletter



A Cautionary Tale: Insurance for Social Engineering Fraud

By: Angela Elbert

You are on the accounts payable staff of a private company. It is 4:30 Friday afternoon, and you receive an urgent email from the CEO (Mrs. Banks). In this urgent email, Mrs. Banks directs you, in no uncertain terms, to immediately wire $750,000 to pay a very important bill before the close of business. You try to reach your boss, but she is gone for the weekend. You try to reach your boss' boss, the CFO, who is not answering his phone. Last, you take a deep breath, swallow, and call Mrs. Banks directly to verify the request; you reach her voicemail. You look closely at the email and it looks totally legitimate. It is now 4:55 p.m., so you swallow even harder and wire the money hoping it was a legitimate request and go home for the weekend. It turns out you were scammed.

Now imagine that your job entails paying your company's vendors. One vendor sends a seemingly routine email asking that future payments be made to a different account. You know the vendor is legitimate and you regularly talk to the vendor's employee who changed the payment instructions. The next week you call the employee and receive her out of office greeting, saying she is on vacation until after the bill is due. To avoid a late fee, you go ahead and pay the bill and send it to the new routing address. Unfortunately, your regular contact didn't send the email. Another scam.

Last, imagine that you are directed to wire your clients' money (which you hold on their behalf) to pay one of their invoices, as you routinely do, but this directive is from a new vendor and is sent directly to you for payment from your client, and you pay it. Scammed again.

All three of these hypotheticals qualifies as a "social engineering" threat. And if something similar has happened to you, you're not alone.

On October 16, 2018, the Securities and Exchange Commission issued an investigative report about the seriousness of these threats and the importance of implementing strong internal accounting controls. The SEC report covers nine undisclosed public companies that were duped out of nearly $100 million as a result of social engineering frauds, most of which was unrecoverable.

Such incidents have been occurring for a few years -- the FBI estimated that social engineering fraud has cost companies more than $5 billion since 2013, greater than losses caused by any other type of cyber-related crime -- but the SEC report should serve as a wakeup call for companies. Companies should prepare by having the right internal accounting controls in place and the right insurance. But what type of insurance is most likely to cover the scams perpetrated in the above hypotheticals?

Given the above scenarios outlined hacks into and cloning of a CEO's email, a vendor's email, and a client's email, your first thought may be cyber insurance. Many cyber-insurance forms, however, principally address data breaches, not social engineering frauds. Without a social engineering endorsement to your cyber policy (which may provide only a small sublimit), your most likely source of coverage would be from a Financial Institution bond that has a social engineering endorsement. These endorsements can be added to a Financial Institution bond for additional premium – but you are often required to complete an additional application that details your internal controls and procedures for detecting fraud. Often, just filling out the application will help you identify where your procedures could use strengthening.

The sublimits initially offered for these endorsements are often inadequate. You should seek higher limits from the insurance company and try to obtain the greatest limits possible, seeking full limits at the primary level, and determine if your excess coverage, if any, will add additional limits. You also must make sure that the endorsement carves back existing exclusions in the policy, such as any voluntary payment exclusion, given that a social engineering payment is akin to a voluntary payment by your employee.

Social engineering endorsements can offer coverage for loss resulting from the insured having paid money as the direct result of a social engineering fraud instruction, often defined as an instruction which intentionally misleads your employee, through misrepresentation which is relied upon by your employee, for the purpose of transferring your money communicated by a director or officer of your company or other authorized employee, or an employee of a vendor authorized by the insured to transfer funds or change bank account information of a vendor, but which instructions were not actually made by such person.

This type of endorsement may provide coverage for the first two hypotheticals, up to the sublimits provided and above the deductible amount. The first two hypotheticals may also cause the company to re-evaluate its internal controls and procedures to see if these instructions were legitimate, and if no voice verification is actually received, whether the funds can be released. They probably should not have been released in either hypothetical – better to make the CEO mad (although Mrs. Banks would be elated that you did not wire the money in the first hypothetical above) or incur a late fee on the vendor bill than to be scammed out of the money. The company should also consider conducting further training with the accounts payable department to make sure that they clearly understand the better option for them in this sort of scenario is to wait to make payment.

So, is there any insurance available to Financial Institutions to purchase for the third hypothetical? Often social engineering endorsements cover losses incurred by your employees who are tricked into giving away your company's money, but they generally do not include when your employee is duped to give away your client's money, such that your client experiences a loss. There is a newer form of endorsement available today that can be added for this specific form of social engineering claim – and it should be added if you are handling your client's money. That endorsement can add coverage for fraudulent transfer instructions relating to your client's money. It can include coverage for loss resulting directly from the insured having, in good faith, transferred your client's money, in reliance upon a fraudulent instruction transmitted to you via email; provided, however, that your employee verified the instruction pursuant to your pre-set procedures and the sender was not authorized to act on behalf of such client.

continued.

This endorsement should be of particular interest to Broker/Dealers and other financial services firms, and this sort of coverage may also be available to these entities as an extension to their errors and omissions policies, at a sublimit and a lower retention. However, you should note that this type of endorsement requires you to jump through quite a few hoops to qualify for coverage, for example procedures to make sure your employees have verified these sorts of instructions pursuant to pre-set procedures, verify that your employees call back a predetermined number as set forth in a written agreement between you and your client and maintaining a contemporaneous record of the call back pursuant to your procedures. But, if those requirements were all met in the third hypothetical, you may be able to obtain coverage for this claim over the deductible and up to the sublimits of coverage available. Again, having an endorsement like this requires that you look closely at your internal control procedures and make sure that those procedures closely track the requirements of this endorsement, so that you can potentially qualify for coverage in the event that you are still scammed. If you handle your client's money, it is important to consider purchasing this form of coverage.

Comments suggestions or inquiries are welcome and should be directed to:
mary.pat.fischer@aon.com

Aon, Inc.

One Liberty Place, 165 Broadway New York, NY 10006 • (800) 243-5117

About the Author

Angela Elbert is the chair of the Insurance Policyholder practice at Neal Gerber & Eisenberg, LLP, in Chicago, IL. She counsels corporate policyholders on complex risk management and insurance issues and develops custom strategies to maximize recovery when claims arise. With over two decades of experience, Angela has been instrumental in recovering hundreds of millions of dollars of insurance for her clients through negotiation, mediation and, where necessary, litigation. Her nationwide risk management practice spans a broad range of capabilities, including negotiating insurance with the best terms available, providing strategic assistance on the insurance aspects of complex corporate transactions, resolving financial insolvency concerns and evaluating, preparing and enforcing indemnification agreements. See https://www.nge.com/Our-Lawyers/Angela-Elbert for more information. Angela can be reached at aelbert@nge.com or (312) 269-5995.