Insurance Law

Social Engineering Insurance Vital for Capital Projects

By Kenneth Rubinstein and Eric Horner

Cyber fraud continues to be a growing problem with real and practical consequences. In response to these growing threats, the insurance industry has developed a solution to protect against the impacts of this new and increasing risk.

Social Engineering Insurance protects companies from confidence schemes in which a bad actor defrauds an employee into sending money or payment on the company's behalf. Today's cyber criminals have moved past the "Nigerian Prince" scam and now employ complex strategies that are effective enough to defraud highly sophisticated companies and institutions. For example, the following story is a real loss on a recent construction project (with only minor details changed to protect the client's identity).

A large New England hospital hired a nationally known contractor to construct a roughly $40,000,000 project. Midway through the project, the hospital's accounts payable manager received an email from someone they thought was their contractor, instructing that the contractor had changed banks, and providing new wiring instructions. The email looked real in every respect. The manager even called the executive's assistant (using the phone number listed on the email) who sounded very professional, answered the phone using the contractor's name, and confirmed the new information.

> "Even sophisticated businesses with strong employee training, employee background checks, and vigorous prequalification can be duped."

Unfortunately, the "assistant" was not actually employed by the contractor and this was part of an elaborate, but increasingly common, scheme. In this instance, the manager followed the instructions, and the contractor did not contact the hospital until two payments had been missed — not wanting to be pushy. By that point, the hospital had wired out approximately $1.5 million in requisition payments.

Even sophisticated businesses with strong employee training, employee background checks, and vigorous prequalification can be duped. Criminals discover an ongoing capital project through print or online media and determine the identity of contractors from media reports, job signage, or otherwise. The criminal then creates a false email account that "spoofs" the actual email address of the company using a similar domain. Accordingly, if the contractor's name is AAA Builders, and their correct email suffix is @aaabuilders.com, the criminal may create and register a domain of aaabuilders.com (using capital I instead of lowercase L) or @aaa-builders.com (inserting a dash in the name) from which to send the email. The criminal then sends the email with the spoofed address (usually using a name that the owner will recognize from the project) to the owner, requesting changes to the payment method. The email often requests that future payments be wired to a specific account number, which is actually the criminal's account. In most instances, victims do not realize they have been defrauded until they are contacted by the real intended payee who never received the required payment. By this time, it is usually too late to recover the funds.

These losses are not covered under standard general liability insurance policies, which generally cover physical losses or bodily injury to third parties. Crime Insurance Policies and Computer Fraud Policies also generally don't cover these losses, even though one might expect them to apply. The Crime Insurance Policies contain various coverage exclusions, such as the "Voluntary Parting Exclusion," which precludes coverage where the insured voluntarily handed over the funds (even where induced through fraud). Likewise, most Computer Fraud Insurance policies generally cover only "unauthorized entries" such as hacking. They do not apply to computer fraud occurring via email as the email by its nature is deemed an authorized "entry."

In response to this coverage gap, many insurance carriers now offer Social Engineering Insurance Coverage to protect against losses stemming from vendor, supplier, and even client impersonation. This insurance is available as an endorsement on a company's existing insurance program, or as a stand-alone coverage option. As with all insurance, significant exclusions and limitations may apply and the specific words of the policy matter. Therefore, companies should review their policies carefully and consult with legal counsel or an insurance professional. That said, Social Engineering Insurance is becoming increasingly common and essential for companies who make significant expenditures, such as capital projects or regular equipment or materials purchases.

Kenneth Rubinstein, an attorney, is co-chair of Preti Flaherty's Construction Law Practice Group and can be reached at KRubinstein@Preti.com.

Eric Horner is a Vice President and Partner at the Rowley Agency and can be reached at EHorner@RowleyAgency.com.