Brown & Brown

PROPERTY & CASUALTY

The Ins and Outs of Social Engineering Coverage

By, Huntley Jackson, Jessica Slater and Michael D'Ambrise

Imagine a CEO receiving an urgent call from their finance department because an employee received an email from a sender they believed to be a company officer. The sender requested payment, and the employee granted it. However, that company officer says they never sent the email.

This scenario is likely a social engineering attack. Bad actors' creativity and ingenuity are endless. Entry points into organizations can be as simple as a one-letter differential in an email address going undetected or a person disguising their voice on the phone to make the request seem authentic. Whatever the method, once an employee initiates a wire transfer and the money has been moved, companies and banks are often left empty-handed.

To help mitigate risks surrounding social engineering, companies can purchase insurance products assisting this type of loss. A comprehensive crime or cyber policy may include social engineering coverage to address the loss in the above scenario. There are considerations to review to help maximize potential coverage.

Callback Provision

Many standard crime policies require any employee receiving a request to transfer funds to make an "out-of-band" callback verification. This means a call is placed using a previously validated phone number to reach the requestor. In the scenario, the employee would have made an internal call to the company officer to determine the authenticity of the request before issuing payment. Coverage is typically limited or excluded if a phone call is not made when a policy has such a requirement.

Vendor or Other Requirements

Other policies require that the falsified request for funds come from a purported vendor or customer of the insured organization. Coverage could be precluded if the bad actor impersonates someone other than a vendor or customer and transfers funds. **Some cyber policies limit who the bad actor purports to be in an otherwise covered social engineering loss.**

Mode of Communication

Certain cyber and crime policies require fraudulent instructions to be provided through a specific mode of communication such as phone, email or facsimile. Coverage can be limited based on how the bad actor conveyed the request. This is significant, given the increase in deep fakes using artificial intelligence (AI) technology.

Coverage Section Nuances

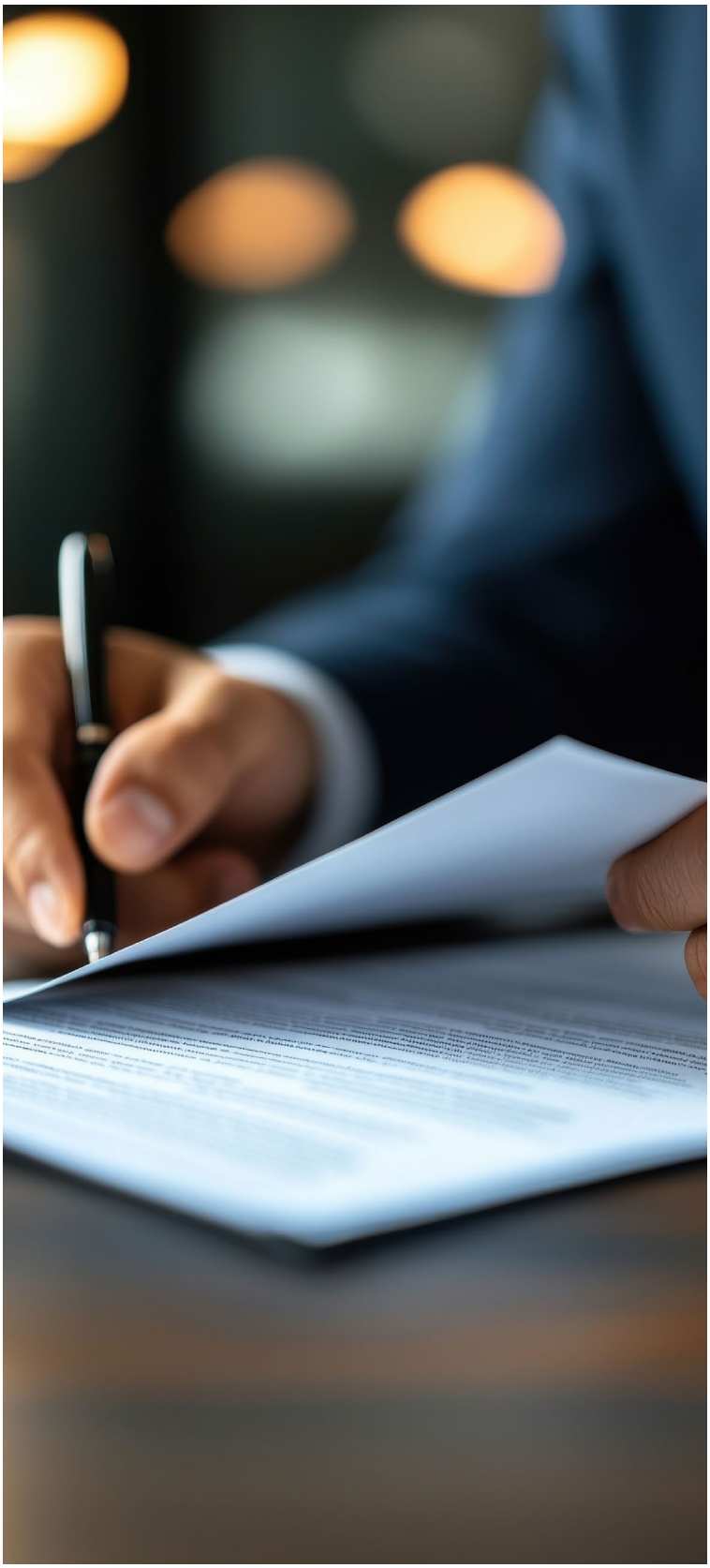
Many crime and cyber policies have a social engineering insuring agreement either built into the base form or added by endorsement. However, there is often confusion around other insuring agreements involving the transfer of funds. Crime policies, for example, characterize losses involving the movement of funds as “funds transfer” or “computer transfer.” The fact pattern of a loss determines which insuring agreement is triggered based on factors such as the entry point of the bad actor, how funds were comprised and whether or not an employee or others were involved.

Policy Overlap

A comprehensive review of all policies potentially providing social engineering coverage is critical for discovering possible gaps in coverage and whether an organization could be uninsured or underinsured. It is not uncommon for both a crime and cyber policy to provide coverage for social engineering. Reviewing policies with potential overlap while considering factors including breadth of coverage, retention differences, pricing deltas and insurance provisions (such as other insurance clauses) allows our customers to align their risk transfer strategy with an informed purchasing decision.

With the continued rise in social engineering losses, businesses may wish to ensure adequate coverage. Given the publicity of these incidents, companies should stay proactive and alert. Cyber and crime liability coverage can assist companies seeking to mitigate risks presented by the threat of social engineering losses.

As business, insurance and technology communities monitor for incidents, companies should carefully assess the effects of a potential social engineering loss and determine if their policies address the incidents as broadly as possible. A trusted broker can help companies seeking to limit the risk with the proper insurance coverage.



How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.

Brown & Brown

Find Your Solution at BBrown.com