COVERAGE INSIGHTS

Social Engineering Fraud Coverage

Marshall & Sterling INSURANCE

Social engineering fraud (SEF) is a type of fraud that's become increasingly common over the last several years. However, even though many instances of this fraud transpire over email communications, it's a company's crime policy—not a cyber policy—that would often provide coverage in the event of an SEF loss.

That's why it's especially important to understand your crime policy, how it might cover SEF, why it might not, and what endorsements you might want to obtain to make sure SEF doesn't leave your company exposed.

Cyber Policy vs. Crime Policy

It may seem counterintuitive, but SEF is usually **not** covered by a cyber policy. Even though this fraud often involves emails and wire transfers, cyber policies are not designed to cover them:

- **Cyber policies** cover losses that result from unauthorized data breaches or system failures. SEF actually depends on these systems working correctly in order to communicate with an organization's employees and transfer information or funds.
- **Crime policies** cover losses that result from theft, fraud or deception. Because the underlying cause of a loss in SEF is **fraud,** a company would claim a loss under its crime policy rather than its cyber policy.

How Social Engineering Fraud Works

There are a number of variations on the theme, but most instances of SEF involve the following elements:

- **A targeted approach**. Criminals will research their targets, purchase authentic-looking domains, manufacture email chains and even resort to making phone calls, all in an effort to make their requests seem authentic.
- **A request.** The preparation is in service of obtaining something from the target, either money (usually in the form of a wire transfer) or information (such as a list of vendors, W-2 information, routing numbers, etc.).
- **The application of social pressure.** In order to bypass in-house safeguards and redundancies, the criminals apply pressure by imposing a time constraint, demanding secrecy or simply flattering the ego of the target by including him or her "in" on an important business transaction.
- **The disappearance of the hacker.** Once the criminals obtain what they want, they disappear with the information or money—things that the company won't miss until it's too late.

Areas of Cover

A standard crime or fidelity policy contains a few provisions under which an SEF claim might be filed:

Social Engineering Fraud Coverage

- **Computer fraud**. This refers to losses stemming from the unlawful theft of money due to a "computer violation"—that is, the unauthorized entry into or deletion of data from a computer system by a third party.

- **Funds transfer fraud.** This refers to losses stemming from fraudulent instructions to transfer funds made without the insured's knowledge or consent.

Potential Vulnerabilities

Depending upon the specific language and definitions laid out in the crime or fidelity policy, the insurer might argue that SEF is excluded from coverage for a number of reasons:

- **There was no "computer violation."** Often, SEF doesn't involve compromising network security in order to steal data. Instead, criminals "hack" human vulnerabilities in order to gain access. Because the system functioned as it was supposed to, and the criminal gained access due to human failure, an insurer might try to deny the claim.

- **The insured knew about and consented to the transfer.** Again, it depends on the specific language of the policy, but an insurer might argue that a SEF isn't covered under "funds transfer fraud." That's because, in most social engineering scenarios, some agent of the insured willingly and knowingly authorized the transfer of funds to the intended account. Again, in SEF, the systems in place to transfer funds worked as intended; it was a human failure that resulted in the loss.

- **The voluntary parting exclusion.** Most crime policies have a voluntary parting exclusion that excludes coverage for losses that result from anyone acting on the insured's authority to part with title to or possession of property. In other words, because the employee knowingly and willingly authorized the transfer, it wouldn't be covered.

Social Engineering Fraud Endorsements

Because of this potential gap in coverage, some carriers have started offering SEF endorsements to their crime and fidelity policies. The insurance agreements might go by different names, but they're all intended to make limits and liabilities explicit for both the insured and the policy issuer.

These endorsements are only offered by a handful of carriers, but with the increasing prevalence of SEF, more are likely to follow. To learn more about SEF, we have resources available for you. Ask about our "Risk Insights: Social Engineering" as well as "Risk Insights: The Fake President Fraud."

And, to discuss your coverage options and learn what options are available to you, contact Marshall & Sterling, Inc. today.