INSIGHTS
RISK & INSURANCE

Companies Are Facing New Types of Digital Theft. Here's How They Can Better Protect Themselves.

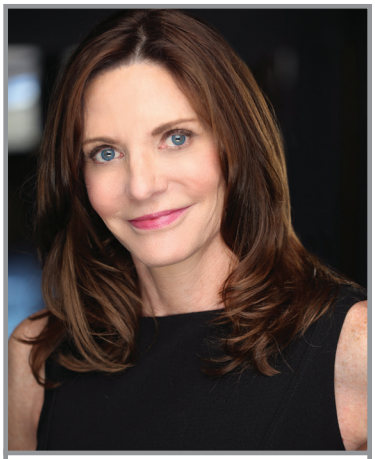
The Hanover Insurance Group

In an increasingly volatile specialty market, agents can create mutually beneficial partnerships with multi-line carriers to help enhance their competitive position in the market.

Crime risk is one of the most dangerous threats to small and mid-sized businesses. Theft can be committed by an employee or a third party outside the organization via traditional means—like employee-run check tampering and payroll schemes—or digitally, like third party phishing scams and other social engineering fraud.

Amid the COVID-19 pandemic, the risk of social engineering fraud may become even greater as more employees work remotely and the usual chains of communication with colleagues are disrupted. And schemers may look to take advantage of workers' increased stress levels. Inundated with negative news and trying to balance work and life in the same space, anxious employees may be more likely to make mistakes.

Social engineering scams – also called business email compromise (BEC) or phishing – have been on the FBI's radar for years and, despite being easily preventable, continue to rise in frequency and severity.



Helen Savaiano, President of Management Liability, The Hanover Insurance Group

The FBI reported a 100% increase in identified global exposed losses stemming from social engineering schemes between May 2018 and June 2019. Between the summers of 2016 and 2019, this type of fraud caused $26 billion in global losses.

Sophisticated thieves, who take time to study a target's chain of command, key vendors and suppliers, level of stringency surrounding accounting procedures, and methods and style of communication, can make off with millions in a single heist. And every type of organization has been targeted – public entities, nonprofits, small private companies and large financial institutions.

"Traditionally, though, crime risk has always been one of the biggest stressors for small- to medium-sized businesses in particular, because economically it's just harder for them to take a hit," said Helen Savaiano, President of Management Liability at The Hanover.

The increased frequency and severity of these schemes has given insurers pause. Here's how the industry is responding to the ubiquity of social engineering fraud, what that means for insureds, and how they can better protect themselves with the right resources.

How Insurers May Respond to the Growing Threat

Historically, many fidelity & crime and cyber insurers covering social engineering fraud for small- to medium-sized enterprises (SMEs) have offered sizable limits with minimal retentions or deductibles. With frequency rising so sharply, the losses may soon become unsustainable.

In response, some carries have started to demand more rate, pulling back capacity and/or tightening terms and conditions.

"There was a period where coverage for this risk was extended with limited questions asked. Now it's fair to say there's more inquiry going on to affirm that risk management procedures are in place. Additionally, many of the carriers in the middle market segment are pulling back on their willingness to offer limits above $250,000. For the small middle market segment, limits around $25,000 to $50,000 may become the new normal," said Savaiano.

"Increasing retentions or pursuing a coinsurance structure so the policyholder has more skin in the game is another option that may drive needed behavior change and loss avoidance," said Steven Vardilos, Vice President, Fidelity & Crime, The Hanover Insurance Group.

Steven Vardilos, Vice President, Fidelity & Crime, The Hanover Insurance Group

While most carriers already stipulate that protocols must be in place to verify the authenticity of wire transfer requests, some may go a step further and require documentation that these protocols were followed in order to receive a full payout. Failure to follow verification procedures could result in only partial recovery.

The bottom line is that companies will be best served by stepping up efforts to prevent losses in the first place.

Both Simple and Complex: The Psychology of Social Engineering

The conundrum of social engineering fraud is that losses are both easy and difficult to prevent at the same time.

Simple procedures can prevent fraudulent transactions from ever being initiated. Calling the source of a request directly at a known phone number, for example, can quickly determine its veracity. Companies can also require a senior manager to approve one-off transfers or changes in payment accounts or schedules. These simple steps would likely nip most scams in the bud. So why aren't they followed?

The reason this type of theft is so successful is because it preys on the vulnerabilities of human psychology. Social engineering scammers take advantage of our natural desire to be good at our jobs, to respond quickly to apparently urgent requests, and to avoid potential conflict that could stem from questioning a request from a supervisor.

"With employee theft, you can establish protocols like segregation of duties and second-level approval on reconciliation of accounts. These things help prevent willful malfeasance from taking place, but those traditional controls don't work when the theft is perpetrated through trickery and the loss of funds is inadvertent," Vardilos said.

Avoiding mistakes may seem simple on the surface, but changing longstanding behaviors and habits is never an easy fix.

How Employers Can Better Protect Themselves

While having verification protocols clearly documented and accessible is the best first step, organizations have to drive cultural change that encourages employees to actually follow those procedures.

"It's just not enough to have good policies. These have to be continually revisited, updated in light of any recent incidents, and retrained. They have to monitor to ensure adherence. Good policies need to be a living, breathing part of your organization," Savaiano said.

Executing this requires understanding and modifying the thought processes and motivations that lead to mistakes.

"You have to start to redefine what competency is. Maybe it's slowing down instead of working faster, and stressing accuracy over speed. If you can change that expectation, then it reinforces for employees that it's okay to double check those requests even if they are marked urgent or come from a senior person," Savaiano said.

Partnering with the right carrier can give risk managers access to the expertise and tools needed to drive this shift.

The Hanover offers a variety of resources designed to help clients mitigate all kinds of theft. This includes a free e-learning course on mitigating social engineering fraud, cyber scam awareness videos, and a bulletin that employees can pin to their work stations reminding them of the telltale signs of a fraudulent email and how to verify a payment request.

The Hanover also maintains a dedicated team of fidelity and crime specialists, each with an average 20 years of experience.

"Many other carriers have combined executive liability with crime, and it's part of a multifaceted approach. We have a very specialized group who focus only on crime risk. They're also located regionally, so they understand the local environment and can address clients' specific concerns and exposures," Savaiano said.

"Our underwriters are specialists in their craft, meaning they're well-versed in the coverages, the exposure, and in identifying good risks from bad risks. That expertise offers a ton of value because there's not a lot of knowledge out there when it comes to crime, and we are able to answer agents' and clients' questions," Vardilos said.

Using both proprietary forms as well as ISO forms, the fidelity and crime underwriters are able to craft coverage custom to any organization's exposure, including private companies, nonprofits, and government bodies. That includes not just social engineering risk, but traditional exposures like employee theft and robbery.

The result is a risk transfer solution that not only protects companies from all types of crime, but also arms them with the knowledge and tools to avoid incidents in the first place.

To learn more, visit https://www.hanover.com/business-insurance-management-liability-fidelity-crime.html.

&BrandStudio

This article was produced by the R&I Brand Studio, a unit of the advertising department of Risk & Insurance, in collaboration with The Hanover Insurance Group. The editorial staff of Risk & Insurance had no role in its preparation.