Beazley Insight

Don't Be Fooled: Cyber Masquerading is a Very Real Commercial Crime Threat

by Bill Jennings

Don't Be Fooled: Cyber Masquerading is a Very Real Commercial Crime Threat

by Bill Jennings

"Computer crime" is not what it used to be. For decades, commercial crime insurance policies were written contemplating the threat of a hacker cracking into a computer network to score an unauthorized transfer of funds - the cyber equivalent of a thief in the night. Today, one of the most prevalent threats is more direct: Thieves can even come right to the "front door," or masquerade online as a senior executive, vendor or other trusted associate of a company – tricking an employee into handing over company assets.

This commercial crime exposure is not one that can be addressed simply with state-of-the-art network security, like the computer hacking crimes of the past. Cyber-masqueraders prey on human nature – using trust, an air of authority, and an employee's desire to please the boss to their advantage.

Unveiling the Exposure

The abundance of information available these days on LinkedIn, Facebook and other social media makes it easier than ever for an individual to collect personal information on executives and employees, so they can use it to convincingly perpetrate this fraud. Often, thieves will begin testing the waters with small amounts of money, moving to larger amounts as no alarm bells ring at a company and the scheme progresses. More often than not, fraudulent instructions direct the victim to send funds to an overseas account – which can make recovering lost assets difficult, if not impossible.

The threat plays out similarly in companies of all types and sizes. We have seen many examples come through our doors. For example, a company's finance director receives an urgent email that is by all appearances from the company's CFO, who is on vacation in the Bahamas (information easily gleaned these days from social media). The CFO explains that funds must be wired immediately to complete a confidential business deal. The finance director wires the funds and later learns that the request did not come from the CFO after all.

Based on an authentic-looking email, another fraudster, posing as a vendor, convinces an employee at a manufacturing company to wire invoice amounts due to the vendor's "new bank account." The employee updates its wire transfers instructions accordingly. The fraud is not discovered until weeks later, when the real vendor contacts the company seeking payment.

Addressing the Risk

Combating this online, one-on-one deception can be difficult. The first line of defense for every company is its employees, who should be actively trained to understand and identify these schemes. Companies should also have prudent verification processes in place, such as requiring out of band authentication of a request before funds are transferred.

Insurance can also help. Beazley is helping commercial crime policyholders safeguard against this newest threat by providing fraudulent instruction coverage. This is an enhancement to our standard commercial crime policy, and addresses losses that result directly from an insured transferring, paying or delivering money or securities as a result of fraudulent instructions provided by someone purporting to be one of the company's vendors, clients or authorized employees.

With this enhancement in place, insureds can be confident that their commercial crime coverage is keeping pace with the exposure that comes when fast-advancing technology converges with unchangeable human nature … and an employee, only doing their job, falls victim to a cyber masquerade.

Bill joined Beazley in July 2010 to establish a Fidelity & Crime underwriting discipline. He has more than 35 years of experience underwriting financial fidelity and commercial crime insurance.

Bill Jennings
Crime Underwriter
New York, NY
bill.jennings@beazley.com

CBSL387_US_06/15

beazley