NEAL GERBER EISENBERG

INSURANCE POLICYHOLDER ALERT

High Profile "Phishing" Incident Demonstrates Continued Need for "Social Engineering" Insurance

March 11, 2020

Media outlets recently reported that Barbara Corcoran, one of the judges on the popular ABC show "Shark Tank," was the victim of a "spear phishing" scam.[1] "Spear fishing" is a form of "phishing" in which someone sends an e-mail to a company employee pretending to be a trusted source, either to obtain money or access to the company's computer system.[2] In Corcoran's case, the scammer pretended to be Corcoran's assistant and sent an e-mail to her bookkeeper asking for nearly $400,000 for a renovation payment for some property. The scammer imitated the assistant's e-mail address and misspelled it by one letter. No one caught the mistake and the money was wired to the fake e-mail address. Fortunately for Corcoran, the bank used for the transfer froze it before the money could be deposited into the scammer's bank account in China.[3]

Corcoran's near miss notwithstanding, such scams are all too common. The Wall Street Journal reports that in 2019, the FBI received 23,775 complaints of business e-mail and e-mail account scams, up from 20,373 in 2018.[4] The annual estimated losses also increased, from $1.2 billion in 2018 to over $1.7 billion in 2019.[5] The number of complaints and amount of losses are likely significantly higher, given that many companies do not report when they have been the victims of such scams.[6] The newspaper further reports that scammers are becoming more sophisticated and are continually coming up with new versions of phishing scams.[7]

When cyber liability insurance first came out, it focused on insuring businesses from losses caused by unauthorized access to consumers' personally identifiable information: credit card numbers, health information, etc. Bigger enterprises with large amounts of such data were seen to be the primary targets of efforts by "hackers" to obtain this data. Smaller businesses and those that do not interface directly with consumers consequently did not necessarily see the need for cyber insurance. Now, however, every business that operates by e-mail (i.e., every business), is at risk of being a victim of e-mail scams. As Corcoran's experience shows, business savvy is no guarantee of protection.

Fortunately, insurance exists that protects businesses from phishing and other "social engineering" scams. Most such insurance is not sold as a stand-alone product, but rather can be purchased as part of a cyber liability or fiduciary/crime policy for an additional premium. Not all such coverage is created equal, however.

---

1 Valinsky, Jordan. "Shark Tank host loses $400,000 in a scam." *CNN*, February 27, 2020, https://www.cnn.com/2020/02/27/business/barbara-corcoran-email-hack-trnd/index.html.

2 "What is Spear Phishing? - Definition." *Kaspersky*, https://usa.kaspersky.com/resource-center/definitions/spear-phishing.

3 Valinsky, Jordan. "'Shark Tank' judge Barbara Corcoran gets her $400,000 back from scammers." *CNN*, March 3, 2020, https://www.cnn.com/2020/03/02/business/barbara-cocoran-email-hack-money-returned/index.html.

4 Ramey, Corinne. "Email Scams Get Savvier, Target Businesses." *Wall Street Journal*, February 28, 2020, at A2.

5 *Id.*

6 *Id.*

7 *Id.*

There is no standard form of social engineering insurance and the terms and limitations can vary widely. For example, some policies require the insured to have followed "callback verification" or other security procedures prior to wiring the money.[8] Other policies limit coverage only to e-mails that purport to have been sent from certain specified individuals or entities – e.g., company executives or vendors or clients – or require the e-mails to have been received by employees who are responsible for processing requests to transfer money. When considering purchasing social engineering coverage, an insured may find it beneficial to consult with professionals – attorneys and brokers – who can assist them in negotiating for favorable terms that will stand up in court in the event of a coverage dispute.

There is little in the way of published case law discussing or interpreting social engineering insurance, but what there is suggests that insurers are prepared to dispute claims. One example of the lengths to which insurers will go to deny claims can be found in *Principle Sols. Grp., LLC v. Ironshore Indem., Inc.*, 944 F.3d 886 (11th Cir. 2019). That case involved a loss of over $1.7 million in a phishing scheme in which scammers posing as one of the insured's executives and an outside lawyer persuaded the controller to wire money to a foreign bank account. The Eleventh Circuit rejected the insurer's arguments and held that the insured's crime policy covered the loss.

As much as we all like to think that we would not fall for phishing scams, the reality is that many of us will at some point. Therefore, it is best to be prepared for such eventuality by at least considering social engineering insurance. Experienced coverage attorneys can assist insureds in negotiating the insurance, and those same attorneys can help resolve claims in the unfortunate event that they occur.

---

8 *Johns Hopkins Fed. Credit Union v. Cumis Ins. Soc'y, Inc.*, No. RDB-09-2009, 2010 U.S. Dist. LEXIS 29351, at *4-5 (D. Md. Mar. 26, 2010).

• • • • • • • • • • •

This alert was authored by Paul Walker-Bright (312-269-8029, pwalkerbright@nge.com).

If you have any questions related to this article or would like additional information, please reach out to your contact in the Insurance Policyholder group or the author.