The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2016
PHILADELPHIA, MONDAY, JUNE 6, 2016
An ALM Publication

E-DISCOVERY AND CYBERSECURITY

Ammunition for Cyberinsurance Policyholders in Phishing Incidents

BY JANA LANDON

Maksim Kabakou/Fotolia

The largest cybersecurity incidents often start by an unwitting employee clicking an attachment to a document or responding to a seemingly legitimate email. The recently released 2016 Symantec Internet Security Threat Report found that one particular type of incident—phishing—has been gaining ground rapidly. Phishing, generally, is a scam by which an email user is duped into revealing personal or confidential information that the scammer then uses illicitly. A typical phishing scenario may be as follows: A CEO sends an email to a human resources employee requesting a PDF of all W-2s for current employees. The HR employee replies to the email, attaching the requested information. However, that information was not requested by the CEO; it came from a hacker, and all of that information is now in the hacker's hands. This type of scam does not involve any complex software, but rather some targeted social engineering, fake email domains, and sometimes even some well-placed telephone calls.

Specifically, Symantec Corp. reported that the legal and finance departments at companies have increasingly been targeted with well-crafted phishing attacks, some of which included wire transfer attempts; successful attacks often cost affected companies millions of dollars, most of which cannot be recovered. For example, Ubiquiti Networks Inc. disclosed late last year that it had been the victim of a phishing attack. Someone impersonating an employee requested wire transfers that resulted in transfers of funds aggregating $46.7 million held by a company subsidiary incorporated in Hong Kong to other overseas accounts held by third parties; the company was only able to recover a little over $8 million. Blogger Brian Krebs reported that phishers made off with $17.2 million from Scoular Co., an employee-owned commodities trader in Omaha, Nebraska—an executive wired the money in installments to a bank in China after receiving emails instructing him to do so. Indeed, the FBI reports that over 7,000 victim companies have lost $750 million in the United

States between October 2013 and August 2015; this form of swindling has grown over 270 percent since January 2015.

There has been, however, a disconnect between this threat and insurance available to cover the risk in the event of a loss. A typical fraud insurance coverage policy contains language covering direct fraudulent transfers, but some insurers have been denying coverage, arguing that a phishing incident—in which an employee is duped into transferring funds—is not the same as a direct hack into a computer system where the hacker causes funds to be transferred. Out of 31 leading cyberinsurance providers, only eight cover fraudulent wire transfer, according to a 2015 cyber and privacy insurance survey by The Betterley Report. Of those eight insurers, the language for wire fraud is often carefully parsed to restrict coverage if the insured is involved in the wire fraud and may have lower coverage limits.

Courts, too, are still working on determining whether or not phishing attacks are covered under fraud insurance policies. For example, there are at least three cases where insureds were denied coverage for phishing incidents (*Medidata Solutions v. Federal Insurance*, No. 1:15cv00907 (S.D.N.Y.); *BitPay v. Massachusetts Bay Insurance*, No. 1:15cv03238 (N.D. Ga.); *Ameriforge Group v. Federal Insurance*, No. 16cv377 (S.D. Tex.) that are currently working their way through the courts, and at least one case from the Southern District of Texas that found coverage for a phishing attack (*Apache v. Great American Insurance*, No. 4:14-CV-237, 2015 U.S. Dist. LEXIS 161683, at *9 (S.D. Tex. Aug. 7, 2015)).

A recent U.S. Court of Appeals for the Eighth Circuit decision provides new support to an insured's position that fraudulent activity by third parties that results in wire transfers should be covered under fraud policies because the fraud was the proximate, although not direct, cause of the loss. In *State Bank of Bellingham v. BancInsure*, No. 14-3432 (8th Cir. May 20, 2016), a bank employee in charge of wire transfers inadvertently left two password tokens in a bank's computer overnight. The computer became infected with malware, and a third party transferred over $485,000 to a foreign bank account. The bank sought coverage for its loss under a financial institutional bond (substantially similar to an insurance policy), but the insurer denied the claim based upon the bond's exclusions for employee-caused losses, theft of confidential information, and a mechanical breakdown or deterioration of a computer system. Upon a summary judgment motion, the trial court ruled in the bank's favor, finding that the efficient and proximate cause of the bank's loss and that neither the employees' violations of policies and practices, the taking of confidential passwords, nor the failure to update the computer's antivirus software had caused the loss. Even if those circumstances had played an essential role in the loss, the court concluded they were not independent and efficient causes of the loss. Importantly, it also found that the proximate cause of the loss was the overall fraudulent scheme perpetrated by the hackers, and that the intervening acts of employees did not make the loss indirect. On appeal, the Eighth Circuit affirmed the trial court's ruling, finding that even though the bond at issue referenced the fact that the loss should not be "indirect," it was not enough to defeat the presumption under Minnesota law that the fraudulent activity was the cause of the loss.

The Eighth Circuit's decision is good news for policyholders because it rebuffs a common argument made by insurance carriers in disputes over fidelity bonds and commercial crime policies: that negligence on the part of a policyholder's employees converts a covered loss caused directly by a third party's criminal acts into an indirect, uncovered loss. When reviewing a company's insurance policies or bonds, it is important to assess changing risks that are facing your client, keep in mind how courts are interpreting key parts of insurance policies for cyberattacks, and engage appropriate counsel to guide you and/or your client through the insurance procurement process. •

Jana Landon *is counsel in Stradley Ronon Stevens & Young's Philadelphia office and founder and chair of the firm's e-discovery team. She litigates complex insurance coverage matters and advises clients on technology issues, including cybersecurity and cyberinsurance. She can be reached at jlandon@stradley.com or 215-564-8049.*

Reprinted with permission from the June 6, 2016 edition of THE LEGAL INTELLIGENCER © 2016 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382, reprints@alm.com or visit www.almreprints.com. # 201-06-16-03