MIAMI-DADE THURSDAY, AUGUST 9, 2018

OFFICIAL COURT NEWSPAPER OF SOUTH FLORIDA
DailyBusinessReview.com
An ALM Publication VOL. 93, NO. 37 $2.00
DAILY BUSINESS REVIEW

PRACTICE FOCUS / INSURANCE

Is Insurance a Safety Net for Phishing or Whaling Attacks?

Commentary by Walter Andrews


Andrews

Just when one thought it was safe to go back into the water companies are being victimized by sophisticated and pervasive social engineering fraud attacks.

"Social engineering fraud" is a broad term that generally refers to computer scams used by cybercriminals to trick their victims into transferring confidential information and funds. "Phishing" is the most common form of social engineering fraud for which the fraudster sends an email impersonating a vendor, client or supervisor of the company and advises that banking information for the vendor/client has changed or company funds immediately need to be wired at the "supervisor's" direction. Such cybercriminals exploit a person's trust in order to find out their banking details, passwords or other personal data. "Whaling" is another term for such attacks when they are made against the top-level executives of companies—the "whales."

Don't think that you are the only one who may fall for these attacks. More than 60 percent of companies report that they have been victims of social engineering fraud and there are well over $1 billion in such losses each year. Companies are doing all that they can to protect themselves from such attacks, but it is clear that insurance should play a major part in protecting companies from such losses.

However, when companies look to their traditional insurance program, they are often told that they do not have coverage for such losses or they learn that they will have to litigate with the insurers to obtain the coverage that the policyholders thought that they had purchased. Insurers have regularly denied coverage for social engineering claims under those policies, claiming that the loss did not result from "direct" fraud. Insurers contend that the crime policy applies only if a hacker penetrates the company's computer system and illegally takes money out of company coffers. In the case of a social engineering claim, company funds have been released with the knowledge and "consent" of an employee, albeit the employee has been induced by fraud to release the funds. Policyholders have prevailed on some of these cases recently, but it takes a long time and a lot of money to get the court to rule favorably. See., e.g., *Medidata Solutions v. Federal Insurance,* No. 17-2492 (2d Cir. July 6 2018); *American Tooling Center v. Travelers Casualty and Surety Co. of America*, No. 17-2014, 2018 WL 3404708 (6th Cir. July 13, 2018).

BOARD OF CONTRIBUTORS

These decisions represent the first times that federal appellate courts have ruled in a policyholder's favor on the direct loss issue in a dispute over coverage for a phishing theft. However, there are other decisions that have gone against policyholders on these issues, including cases that have found that the insured's failure to properly investigate fraudulent emails meant that the loss did not result "directly" from the use of a computer as required by the policies and that steps taken between the receipt of social engineering emails and the eventual transfer of funds broke the chain of immediacy required by the insurance provision at issue. And, while these more recent federal appellate decisions provide guidance on a number of recurring issues under computer fraud policies, it left open the door for debate on key points in future cases, a debate that policyholders should try to avoid because they don't have the same resources that insurers have to tie these issues up in court.

Hijacking or spoofing email addresses should be considered an attack on a company's computer system for which a reasonable policyholder should expect coverage, but that is not always the case. While there should be coverage for these losses they are often denied by the insurance companies. These decisions should serve as a reminder to policyholders to review their cyber and crime insurance policies with experienced insurance coverage counsel to determine whether the specific policy provisions meet each policyholder's particular needs and whether any revisions may be necessary before, or at, renewal to avoid any disputes. If companies are victims of phishing or whaling attacks they should carefully consider the insurance coverage they purchased in order to determine whether they have coverage, including under both traditional insurance policies and specialized cyber insurance products. Don't allow your company to be a potential victim of a phishing or whaling attack without an appropriate insurance safety net.

Walter J. Andrews, a partner at Hunton & Williams, focuses his practice on complex insurance litigation, counseling and reinsurance arbitrations and expert witness testimony.