LITIGATION NEWS

ABA Section of Litigation

TOP STORY

As Cybercrime Increases, Companies Look to Insurance

By Grant H. Hackley – June 25, 2020

As cybercrime grows, companies are looking to insurance policies to minimize losses. The U.S. Court of Appeals for the Eleventh Circuit held, in a divided opinion, that a cybercrime policy covered a $1.7 million loss from a spear-phishing attack. Yet experts suggest that coverage may be nuanced and they advise that clients should examine policies closely and train employees on how to avoid cybercrime schemes.

Spear-phishing does not involve a harpoon. Rather, it is becoming one of the more prolific and effective types of internet crime. Spear-phishing is a fraudulent attempt, usually by email, to obtain sensitive information from or induce activity by a specific recipient. This is done by masking the identity of the sender as someone trustworthy, and typically involves creating a sense of secrecy and urgency. Large businesses are prime targets. According to the Federal Bureau of Investigation's Internet Crime Complaint Center, such attacks accounted for $1.7 billion in losses in 2019 alone. The result is a growing awareness of the risk, and a shift in the insurance coverage landscape.

Spoofed Email Results in $1.7 Million Loss

In *Principle Solutions Group, LLP v. Ironshore Indemnity, Inc.*, the Eleventh Circuit addressed insurance coverage for a loss arising from spear-phishing. Principle Solutions' controller, Loann Lien, received an email from the managing director of the firm stating that he had engaged in secret negotiations for a "key acquisition" and directing her to follow wiring instructions she would receive shortly from an "Attorney Mark Leach." The email urged discretion and told her to give the attorney her "full attention." Five minutes later, Leach emailed Lien wiring instructions for a $1.7 million transfer to a Chinese bank. Lien commenced the transfer, triggering Wells Fargo's fraud prevention services. After a back and forth with Wells Fargo and a phone call with Leach, Lien confirmed the transfer. From start to finish, just over two hours elapsed. Lien learned the next day that the email from the managing director had been spoofed, but by then it was too late; the money was gone.

Principle Solutions sought coverage from Ironshore under a commercial crime policy that covered "[l]oss resulting directly from a fraudulent instruction to a financial institution to debit [Principle's] transfer account, and transfer, pay or deliver money or securities from that account." Ironshore denied coverage. In the ensuing litigation, the U.S. District Court for the Northern District of Georgia granted Principle Solutions' motion for summary judgment, and a divided panel of the Eleventh Circuit affirmed.

What Does the Policy Say?

In analyzing the insurance policy, the Eleventh Circuit focused on the definition of a fraudulent instruction as an "electronic or written instruction initially received by [Principle], which instruction purports to have been issued by an employee, but which in fact was fraudulently issued by someone else without [Principle's] or the employee's knowledge or consent." Ironshore had argued that because the outside lawyer—not someone purporting to be an employee—provided the actual wiring information, the fraudulent instruction did not meet the definition as having been issued by an employee.

The appellate court was unpersuaded by Ironshore's "divide-and-conquer approach" and concluded that "[n]othing in the policy language warrants the assumption that the two [communications] could not be part of the same fraudulent instruction." Similarly, the dissent appeared to agree that the facts were sufficient to establish a fraudulent instruction. However, the dissent suggested that the question of whether the loss was direct and proximate should have been decided by a jury in light of the fraud alert issued prior to completion of the transaction.

What Should a Company or Insurer Do?

Corporations and carriers should beware that coverage for cybercrime tuns on nuanced language. "The insurance policies are written by insurers to respond to a new wave of problems. With emerging risks, different carriers have different language to address new problems," says John B. Mumford Jr., Richmond, VA, former cochair of the ABA Section of Litigation's Insurance Coverage Litigation Committee.

"In *Principle Solutions*, the court was really parsing out what these few words meant," observes Mumford. Indeed, contractual interpretation will determine whether a loss is covered, or litigation successful. On a case-by-case basis, "coverage comes down to what the policy language says," Mumford adds.

As a result, insureds should not assume they are covered by commercial crime or other policies. "Policy terminology is evolving," notes Sean O'D. Bosack, Milwaukee, WI, cochair of the Section of Litigation's Corporate Counsel Committee. "Corporate clients should review their coverage," Bosack says. "My advice is they should ensure they are talking to a very sophisticated broker. They are better off being over-covered rather than under-covered, both in dollar value and scope of coverage," he adds.

Bosack also indicated there are other ways corporations can protect themselves from the risk: "Nowadays, companies can participate in firmwide training to avoid spear-phishing and other attacks," he says. "Sometimes, as a benefit of the insurance premium, carriers and brokers will provide that training, and sometimes carriers will require that the insured certify that the training has taken place," advises Bosack. In the meantime, be careful with that email from your boss.

Grant H. Hackley is a contributing editor for Litigation News.

Hashtags: #spearphishing, #insurancecoverage #cybercrime

Related Resources

- Gregory Wright & Gillian Giannetti, "Insurance Coverage for Business Email Compromise Losses," *Insurance Coverage Committee* (Nov. 20, 2017).