The Remedy for the New Cyber Threat Posing Major Coverage Problems: "Fake President" E-mails

07.10.2017 | By James H. Vorhis

In the last few weeks, we have seen yet another widespread ransomware attack that hit nearly one hundred companies around the world. It reminded me of a recent request from a client, made just after news broke of the WannaCry ransomware attacks, to review its insurance portfolio to confirm that it was covered for ransomware attack. The client had that coverage, but I noticed that there was a gaping hole in the policy for another type of common attack that goes by a variety of names – business e-mail compromise, social engineering fraud, and fake president fraud. What is critical for companies to understand, and few do, is that they must purchase a specific endorsement to obtain this kind of coverage.

These types of attacks are as much identity fraud as they are a cyberattack. In these kinds of cases, an impostor will pose as a high ranking executive at a company, and command a lower level employee via email to wire money to a client or vendor account. The employee, so diligently trained to follow orders, will then complete the transaction, unwittingly transferring company funds into a fake account. After all, what employee would question the company's CEO, CFO, President, or other superior?

This crime poses significant challenges from a coverage perspective. The act does not fit cleanly within the typical first party coverages included in cyber policies – it isn't a data breach, in which information is stolen or compromised and needs to be repaired, and it isn't a ransomware attack, in which a company has its business shut down. These types of attacks also aren't covered by modern crime policies because the action taken – the wiring of money by an employee – is voluntary. There is no extortion, and no money is stolen.

Courts recently confronted with these situations have routinely denied coverage. One example can be seen in *Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am.*, No. C14-1368RSL, 2016 U.S. Dist. LEXIS 88985

(W.D. Wash. July 8, 2016). There, a hacker impersonating a vendor of the policyholder directed an employee to change the bank account for future payments to that vendor. The employee dutifully did so, and the policyholder lost over $700,000 when money was wired to the fraudster's account. The crime policy covered computer fraud, but contained an exclusion for loss resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System. Travelers denied coverage because the employee had authorization to input the new bank information to the account, and the District Court agreed, finding that the loss – the transfer of money to the new account – indirectly resulted from the inputting of the new bank information.

In *Taylor & Lieberman v. Fed. Ins. Co.*, 2017 U.S. App. LEXIS 4205 (9th Cir. Mar. 9, 2017), the Ninth Circuit was faced with a similar situation. There, an accounting firm handled payments and transfers for its clients. An impostor took control of a client's e-mail account and sent multiple wire payment instructions to the accounting firm. The employee wired the money, and did not discover the fraud until the third request to wire money. The accounting firm sought coverage under its crime policy, which provided coverage for direct loss sustained by an Insured. The Court denied coverage because it determined the accounting firm was seeking recovery for third party losses – those of its clients – and not its own. That the company might have to indemnify that client for the fraudulent payments was immaterial.

Fortunately, not all cases end with an insurer victory. But the uncertainty of these results begs the question: how do you insure for these attacks? The answer is a policy endorsement targeted at these types of attacks. It is usually added to a company's crime policy, and will include language such as the Company will reimburse the Insured for Loss sustained by the Insured Person as a direct or indirect result of Business E-mail Compromise. The Policy will then define Business E-mail Compromise, and within that definition it should include reference to coverage for voluntary actions of the insured (who is wiring money under false pretenses). The policy limits for these endorsements tend to be lower than the policy it is attached to, but any coverage an insured can obtain for this kind of fraud is better than none.

There are a few important takeaways on this issue. First, check your insurance policies for language that may suggest coverage in this area, and read the language closely. You will want to make sure your company is covered when money is sent by employees as a result of fraud. If you do not see such language, ask your broker to get you options to add this endorsement to one of your policies. Second, confirm that the policy endorsement you obtain is broad enough to subsume the acts you are seeking to cover. The worst case scenario would be purchasing an endorsement that fails to cover the fraudulent actions for which you are hoping to obtain insurance. Finally, train your employees for these types of situations. A simple 30 minute training on how to identify tells that reveal these schemes may help your company avoid hundreds of thousands of dollars in losses by avoiding this situation altogether.