February 2016 ▪ Volume 21 ▪ Issue 2

Cyberspace LAWYER

CYBER INSURANCE AND SOCIAL ENGINEERING FRAUD, WHY VOLUNTARY TRANSFERS MAY NOT BE COVERED BY YOUR INSURANCE POLICIES

by Thomas H. Bentz, Jr.

Thomas H. Bentz, Jr. (thomas.bentz@hklaw.com) is a partner at Holland & Knight where he practices insurance law with a focus on D&O, cyber and other management liability insurance policies. Mr. Bentz leads Holland & Knight's D&O and Management Liability Insurance Team which provides insight and guidance on ways to improve policy language and helps insureds maximize their possible insurance recovery.

Introduction

In the last few years, many companies have purchased cyber liability insurance to help cover their risk of computer fraud or attack. However, not all cyber insurance policies are created equal and these policies may have significant coverage gaps if they are not properly negotiated.

One of the more common and costly coverage gaps is the lack of coverage for "voluntary transfers." There are many variations on this scam but essentially, the CFO receives what appears to be a real email from a client or vendor asking the CFO to wire money to an account. The email often looks completely real and, in fact, is often the result of a hacker breaking into the client or vendor's system, allowing the hacker to send messages from the client or vendor's actual email address.

Only after wiring the money (often multiple transfers and increasingly larger sums) does the CFO learn that he or she has become a victim of fraud.

We have seen this scam hit companies large and small and across several industries including banks, manufacturers, retailers and even several law firms. And nearly without fail, all of these companies are surprised to learn that they are not insured against this loss because their policies contain an exclusion that states that there is no coverage for a "voluntary parting" (i.e., where the insured voluntarily transfers money to a third party). This exclusion applies even though the CFO was tricked into wiring the money.

The most frustrating and unfortunate part of this situation, is that coverage for this type of social engineering fraud is generally available upon request. Moreover, there is usually only a nominal additional premium required for the coverage. It is just that most companies do not know to ask for it.

THOMSON REUTERS

What You Should Do Now to Protect Your Company

1. Talk to your insurance broker about social engineering coverage today.

As noted above, social engineering fraud coverage is generally available upon request and without a significant additional premium. This type of fraud is not going away and even the strongest controls can be breached. If you cannot stop fraud, at least you can minimize its effect.

2. Review other potential gaps in your cyber liability insurance program.

There is no standard cyber liability insurance form which means that the coverage offered by one insurer may (and often does) differ dramatically from that offered by another insurer. There is little agreement between insurers on what should be covered, when the coverage should be triggered or even how basic terms should be defined. These differences make understanding what is and is not covered very difficult. It also makes it nearly impossible (or at least foolish) to purchase this coverage based on price alone.

Companies are well advised to work with an experienced and knowledgeable insurance professional that understands both what coverage is available in marketplace and the types of claims being made on the policies.

3. Understand how your cyber insurance coverage works with your other insurance policies.

Cyber liability policies are not the only place where an insured might find coverage for a cyber event. Depending on the losses and/or allegations, several other types of insurance policies may also respond to a cyber-related claim.

Understanding where there may be coverage for a claim as well as how the various lines of coverage will work together in the event of a claim is imperative to a strong insurance program. Coordinating limits, retentions/deductibles and other coverage requirements may be difficult. In addition, because multiple types of policies may apply, there may be problems coordinating defense counsel (different insurers may not approve of a firm required by another insurer or there may be disagreement between insurers about reasonable hourly rates). The claims made requirement of many of these policies may also present problems for insureds in the event of a claim. Insureds are well advised to coordinate their coverage in advance so they are not attempting to resolve these issues for the first time after a cyber event has occurred.

Conclusion

Cyber insurance is still evolving. Insureds must take the time to learn what coverage they need and what coverage they have to ensure they are adequately protected. In addition, insureds should have a plan in place to deal with the complexity of having multiple lines of coverage that may apply to a single cyber event. A little preparation can avoid significant problems with coverage in the event of a claim.