DO YOU HAVE THE RIGHT CYBER INSURANCE FOR YOUR BUSINESS?

Robert Tugander Rivkin Radler LLP

Businesses today recognize the importance of having insurance to hedge against cyber losses. And as cyber claims increase, so do decisions by courts interpreting cyber insurance policies. But similar crimes under similar policies have yielded different coverage results. Why the different outcomes?

Sometimes the facts differ. Subtle differences in how a crime was committed can have a big impact on coverage. Sometimes, the policy language differs. And sometimes, courts simply interpret similar clauses differently. In many cases, however, the policyholder failed to purchase endorsements that would have covered the specific crime.

A commercial crime policy, for example, may offer protection for Computer Transfer Fraud, Social Engineering Fraud, Funds Transfer Fraud, and Forgery or Alteration coverage, to name a few. And while these coverages may share similar names, they cover different types of losses.

Knowing available coverage options and how courts have interpreted these provisions can help companies decide how to best manage their cyber risks. A few cases decided within the past year are instructive.

FORGERY OR ALTERATION COVERAGE

A Forgery or Alteration endorsement typically insures against losses resulting directly from forgery or alteration of a check, draft, promissory note, or similar written promise.

A recurring issue is whether a fraudulent email directing an employee to wire funds is the type of forged instrument addressed by the Forgery or Alteration endorsement. Most courts have found that it is not.[1] The endorsement limits its coverage to negotiable instruments. An email telling an employee to wire money to a bank account simply does not have the same legal effect as a check, draft or promissory note.

Earlier this year, two courts interpreted this endorsement where the forgery was more intrusive. Instead of just an email duping an employee to send the wire instructions, the thieves hacked into the policyholders' email accounts. In one case, the thieves intercepted emails transmitting real invoices and attached them to a counterfeit email misdirecting payment.[2] In another case, the hackers cut and pasted signatures on wire transfer authorization forms and used the company's email system to send those authorizations to banks.[3]

But these factual differences did not change the outcome. The Forgery or Alteration provision still did not cover the loss. The invoices were not endorsable instruments payable upon tender in the same way as negotiable instruments. And the forged wire transfer authorization form, like a fraudulent email, was not itself negotiable, but merely directed the bank to act.

So then, what coverage is available for losses from fraudulent instructions to wire money?

FUNDS TRANSFER FRAUD/COMPUTER TRANSFER FRAUD COVERAGE

The company that had its invoices intercepted recovered some of its losses because it also purchased Funds Transfer Fraud coverage. These clauses, subject to variation, cover losses resulting directly from the use of a computer to fraudulently cause a transfer from inside the company's building or its bank to a place outside those premises. But a word of caution: Check the limits. The company's Funds Transfer Fraud coverage carried relatively low limits, which caused it to look to the Forgery or Alteration endorsement in a failed attempt to cover the remainder of its losses.

The company victimized by the forged wire authorizations opted not to purchase Funds Transfer Fraud coverage. The company could have eased its pain had it chosen to do so.

What if the wire transfer occurs by way of an email that tricked an employee into sending the funds to the phony account? Do computer transfer fraud provisions cover this situation?

The U.S. Court of Appeals for the Fifth Circuit took up this issue this past February.[4] The insured's CFO received an email attaching a letter from what he thought was a vendor. The email stated that future payments should be routed to a new bank account. The body of the email also contained previous emails between the company and its vendor concerning invoices and shipping details. The CFO authorized two wire transfers totaling more than $1 million, and those payments were made in accordance with the company's three-step verification process. But the email was from an imposter, and the money was lost.

At issue was the policy's Computer Transfer Fraud provision. The court acknowledged that the scammers created a "fraudulent channel" that allowed them to monitor and alter emails sent between the company and its vendor. But the court found that manipulating emails did not constitute Computer Transfer Fraud because the scammers did not introduce data or programs that independently instructed the computer system to "act."

The Computer Transfer Fraud coverage did not apply for another reason. The transfer was not made without the insured's knowledge or consent. Rather, three employees affirmatively authorized the transfer. By adding the knowledge requirement, the court explained, the policy limited coverage only to instances in which the computer itself is tricked into fraudulently transferring funds to a third party without the insured's knowledge.[5]

SOCIAL ENGINEERING FRAUD

The policyholder was not left completely holding the bag, however. The insurer paid the claim under the Social Engineering Fraud provision.

As the Fifth Circuit noted, the Social Engineering Fraud provision covers situations in which an employee relies, in good faith, on a fraudulent instruction. In contrast, the Computer Transfer Fraud provision disclaims coverage for transfers made with the insured's knowledge.

Again, the limits are important. The Social Engineering Fraud coverage had a policy limit of only $100,000, compared to a $1 million limit for Computer Transfer Fraud.

RANSOMWARE

How do these policy provisions apply to ransomware attacks, where malicious computer code renders a victim's computer useless by blocking access to programs and data?

The Indiana Supreme Court recently interpreted a Computer Fraud provision that covered loss "resulting directly from the use of any computer to fraudulently cause a transfer of money" against the backdrop of a ransomware attack.[6]

After being locked out of its computer system, a company paid the hacker's requested ransom with four bitcoin valued at about $35,000. The company believed that the hacker gained access to its system via a targeted spear-phishing email.

The insurer denied the claim. The trial and intermediate appellate courts upheld the denial. The lower courts found that the loss was not due to fraud, but rather theft, and that the ransom payment was voluntary and not directly from the use of a computer.

The Indiana Supreme Court saw it differently. It first focused on the phrase "fraudulently cause a transfer." It found that the phrase was unambiguous and means "to obtain by trick." But the record was sparse, and the court could not determine if the hackers in fact gained entry to the company's computers "by trick." It sent the case back to the trial court to resolve the issue, cautioning that not every ransomware attack is necessarily fraudulent. If, for example, appropriate safeguards are lacking, a hacker could enter a company's servers unhindered.

The court also considered if the loss resulted directly from the use of a computer. Was computer use part and parcel of the entire scheme, or was the voluntary transfer of bitcoin an intervening cause that severed the causal chain?

To answer this question, the court considered if the loss resulted "immediately or proximately without significant deviation from the use of a computer." The court found that there was sufficient causation. In the court's view, the insured consciously made the bitcoin payment but did so under duress. The court saw the bitcoin payment as nearly the immediate result, without significant deviation, from the use of a computer.[7]

After three attempts, the ransomware victim's claim for coverage survived for another day. But all of that litigation, which still did not fully resolve the coverage issue, may have been avoided had the insured not declined the computer hacking and computer virus coverage that was available for purchase.

So, what's the lesson here? Different coverages are available to protect against specific types of cybercrime, but no single coverage provides full protection against all types of cybercrime. A company is wise to take a hard look at its existing insurance policies and determine if its coverage offers adequate protection against many of the common cyber risks. An insurance broker can help fill in any obvious coverage gaps.

1 *See, e.g., Taylor & Lieberman v. Federal Ins. Co.*, 681 F. App'x 627 (9th Cir. 2017); *Metro Brokers, Inc. v. Transportation Ins. Co.*, 603 F. App'x 833 (11th Cir. 2015); *Midlothian Enter., Inc. v. Owners Ins. Co.*, 439 F. Supp. 3d 737 (E.D. Va. 2020).
2 *AIMS Ins. Prog. Mgrs., Inc. v. Nat'l Fire Ins. Co.*, No. 1 CA-CV 20-0032, 2021 Ariz. App. Unpub. LEXIS 123 (Ariz. Ct. App. Feb. 4, 2021).
3 *Ryeco, LLC v. Selective Ins. Co.*, No. 20-3182, 2021 U.S. Dist. LEXIS 91186 (E.D. Pa. May 13, 2021).
4 *Mississippi Silicon Holdings, LLC v. Axis Ins. Co.*, 843 F. App'x 581 (5th Cir. Feb. 4, 2021).
5 *Taylor & Lieberman*, 681 F. App'x at 629.
6 *G&G Oil Co. of Indiana v. Continental Western Ins. Co.*, 165 N.E.3d 82 (Ind. 2021).
7 Causation is far from settled, however, as courts have reached varying conclusions on whether and when a loss is direct.

Robert Tugander is a partner in Rivkin Radler LLP's Insurance Coverage practice.