Tech Challenge: Cyber Coverage

Insight

The Square Peg of Cyber Coverage

When policyholders recognize a gap, insurers should recognize a need.

Cyber-related disasters have become staples of the business news. Nearly every day, we receive a report of a new theft, information release or other cyber problem. Each incident seems to break records for biggest and worst.

As I've repeatedly written in this space, after new technologies create new liabilities, the new liability issues create new insurance issues. This simple principle was again shown in a new case from the U.S. Court of Appeals for the 11th Circuit, *Metro Brokers v. Transportation Insurance Co.*

In the cyber context, we see another pattern emerging. Policyholders try to fit cyber-related losses into standard policies. But courts are often interpreting standard policies literally. Courts are rejecting policyholders' efforts to put the square peg of cyber losses into the round hole of standard policies.

More specifically, in this case the policyholder, Metro Brokers, is a real estate broker. Thieves injected a virus into the policyholder's computer system. This virus allowed the thieves to uncover access IDs and passwords for Metro Broker's bank accounts. With this information, the thieves logged into the policyholder's online banking system and stole more than $154,000.

This claim created two coverage questions. First, was the theft covered by the policy's Fraud and Alteration endorsement? Second, if the claim was within the coverage of the endorsement, was the claim subject to the exclusions for malicious code or system penetration?

Under the F&A endorsement, the insurer covered "loss resulting directly from 'forgery' or alteration of, on, or in any check, draft, promissory note, bill of exchange, or other similar written promise, order or direction to pay a sum certain…." The policy defined "forgery" as "the signing of the name of another person or organization with intent to deceive." Admittedly, the thieves' actions can be analogized to a forgery. But the terms here were defined specifically. Coverage applied to instruments that were "written." There was no "signing." Consequently, the court found that this incident fell outside of the coverage.

The court then wrote that even if the policyholder had established coverage, it would have been excluded under the malicious code exclusion. "Malicious code" was defined to include, among other things, computer viruses. The policyholder argued that the exclusion did not apply because the thieves' intervening act, not the virus, caused the loss. The court interpreted the exclusion more broadly. Since the thieves used a virus to commit the crime, the court would have applied the exclusion for losses "caused directly or indirectly" by malicious code "regardless of any other cause or event that contributes concurrently or in any sequence to the loss."

This case is another indication that courts seem to reject policyholders' efforts to put cyber claims into traditional policies. It's reminiscent of a trend we saw in the 1990s involving employment claims. When employment claims became more frequent, we saw many policyholders trying to find coverage under traditional liability policies. Most courts rejected these efforts. Ultimately, policyholders recognized a gap and insurers recognized a need. Insurers started offering employment practices liability coverage. The new EPL policies applied; the traditional ones didn't. Coverage disputes and cases diminished.

The arc is similar. Now, we are seeing some insurers offer specific insurance products for cyber losses. I suspect sales of these products will go up and cyber-related coverage disputes will go down. BR

By
Alan Rutkin

Gaps emerge when courts reject efforts to put cyber claims into traditional policies.

Best's Review columnist **Alan Rutkin** is a partner at Rivkin Radler in Uniondale, N.Y. He can be reached at *alan.rutkin@rivkin.com*