When It Comes to Cyber Insurance Words Matter

Daily Business Review
10.13.22

This article appeared in the Daily Business Review on October 13, 2022.

Commentary provided by Ella A. Shenhav and Eric S. Adams.

Insurance is everywhere in our personal and professional lives—from liability insurance to pet insurance. Recently, a new type of insurance has entered our lexicon—cyber insurance. Cyber events are increasingly common, and companies are obtaining insurance to protect them.

In several recent cases, companies with cyber insurance discovered that provisions in these policies led their insurers to limit coverage. Courts have been strictly construing cyber policies, and have found that the coverage provided is narrow. These decisions hinged upon whether an event constituted a covered "direct" loss and whether intervening actions precluded coverage, like an employee responding to fraudulent communications.

In February 2021, a Texas federal court determined that a payment processor for rental property management companies was not covered for losses from a phishing event. See *RealPage v. National Union Fire Insurance Co. of Pittsburgh*, Case No. 3:19-cv-1350-B, United States District Court, Northern District of Texas (February 24, 2021). Hackers used a fishing scam to gain access to funds held by RealPage's third-party payment processor, Stripe. RealPage made a business decision to reimburse its clients. The policy required that RealPage "hold" funds as a prerequisite to coverage for any funds stolen through cyber fraud. The insurer denied the claim because, while RealPage could direct the transfer of those funds in the Stripe accounts, RealPage never "held" the funds that were lost.

Last month, a Minnesota federal court determined that there was no computer fraud coverage for a social engineering loss. Social engineering is a term used for certain types of security incidents where malicious actors trick someone into giving away sensitive information or transferring company funds. See *SJ Computers v. Travelers Casualty and Surety Company of America,* Case No. 21-CV-2482, United States District Court, District of Minnesota (August 12, 2022). "Spoofed" emails were sent from an outside vendor to the purchasing manager at SJ Computers. The "spoofed" emails contained updated wire transfer instructions for the payment of the vendors' invoices. SJ Computers paid invoices totaling nearly $600,000, but the payments went to the hackers' bank accounts.

In *SJ Computers*, the insurer argued that, because the fraudulent emails resulted in an employee updating the wire information, the scheme did not fall under the computer fraud policy and the loss was not a "direct" result of "computer fraud," a term strictly defined in the policy. The insurer argued

that the claim should have been made under its social engineering fraud sub-policy, which only provided up to $100,000 in coverage. The trial court agreed that the computer fraud coverage was not triggered, focusing on the underlying policy language, which distinguished between social engineering fraud and computer fraud.

Most recently, on Sept. 6, a federal appellate court affirmed the trial court's decision that there was not insurance coverage where an unknown actor impersonated a mortgage lender. See *Star Title Partners of Palm Harbor versus Illinois Union Insurance,* Case No. 21-13343 (11th Cir. September 6, 2022). The fraudster induced Star Title to wire funds to a fraudulent account. Star Title made a claim against its cyber insurance policy. The insurer denied the claim because the fraudster was impersonating a mortgage lender and the policy only extended coverage if a fraudster were impersonating "an employee, customer, client or vendor." The courts agreed with the insurer's strict reading of the policy that the impersonated mortgage company did not fall within the defined scope of coverage.

What can businesses learn from these recent developments? Cyber insurance policies are replete with terms and definitions, which impact the scope of coverage. Companies should review their current cyber insurance coverages and consider whether additional insurance products may be necessary to address cybersecurity risks. Coverage for social engineering issues is often defined narrowly. In preparation for an "eventual" cyber breach, Companies should meet with their insurance brokers and explore additional cyber insurance products which may provide coverage beyond the traditional computer fraud policy. These products include Business Email Compromise (BEC), invoice manipulation, cryptojacking, telecom fraud, and funds transfer fraud.

In addition to obtaining appropriate insurance, companies should also conduct employee training and maintain robust cybersecurity measures. Despite ransomware making recent headlines, industry experts report that the majority of malicious breaches are due to social engineering and phishing attacks. Privacy and technology professionals recommend that companies use multi-factor authentication and mandate recurring training, with specialized training for those who regularly handle sensitive data. Insurance should not be a company's only protection against cyber events.

Ella Shenhav *is a partner in the Tampa office of Shutts & Bowen, where she is a member of the business litigation practice group and the firm's pro bono committee. She is a Certified Information Privacy Professional (CIPP/US), accredited by the International Association of Privacy Professionals (IAPP). Ella focuses her practice on complex commercial litigation and on privacy and data protection.*

Eric S. Adams *is a partner in the Tampa office of the firm, where he is a member of the business litigation practice group and the construction practice group. He is also chair of the firm's e-discovery committee. He focuses his practice on litigation involving business disputes, construction, trusts and estates, real estate and intellectual property.*

When It Comes to Cyber Insurance Words Matter

Professionals

Eric S. Adams

Ella A. Shenhav

Practice Areas

Cybersecurity and Data Privacy Task Force

Litigation

Offices

Tampa