MAXIMIZING INSURANCE COVERAGE FOR CYBERCRIME LOSSES

BY P. WESLEY LAMBERT

With high-profile cybercrime cases dominating the headlines, policyholders and insurers are engaged in an ongoing struggle behind the scenes to define the contours of insurance coverage for what are often massive losses borne by policyholders and third-parties victimized by these crimes. The increasing frequency and complexity of cybercrimes has naturally led to an increase in the number of insurance coverage actions initiated by and against policyholders demanding coverage from their insurers. While courts nationally attempt to more clearly define the legal issues upon which coverage cases will turn, policyholders would be well-served to keep the following issues at the forefront of their minds when planning for, or responding to, cybercrime risks.

1. Evaluate the types of cybercrimes to which you are susceptible.

Policyholders generally face two categories of risks for which they may ultimately purchase coverage. The first is risk to the policyholder's own property — its computers, data, and financial resources. The second is risk that the policyholder will be liable to third parties if their data is compromised, or if the policyholder is in breach of some other duty to a third party resulting from a cybercrime.

Social engineering schemes have also taken a more prominent role in the cybercrime landscape. Perhaps the most prevalent social engineering scheme, at least as far as the insurance coverage cases are concerned, is the business email compromise (BEC) scheme. Law enforcement agencies have reported seeing BEC schemes perpetrated frequently on businesses that perform regular wire transfer transactions. BEC schemes are often carried out when perpetrators compromise or spoof high-level executives' email accounts to fraudulently direct electronic funds transfers from the company to the hacker's bank account.

2. Policyholders may be entitled to a defense against cyber-related claims.

Under many states' laws, including Ohio's, an insurer's duty to defend is distinct from and broader than its indemnity obligation. Thus, policyholders facing third-party claims resulting from cyber liability should evaluate whether their insurance policy will provide for a defense against such claims even where there may ultimately be little or no indemnification for the third party's loss.

For example, in *Eyeblaster, Inc. v. Federal Ins. Co.*, 613 F.3d 797 (8th Cir. 2010), the Eighth Circuit Court of Appeals held that the policyholder was owed a defense by its insurer against claims that a third-party's computer, software, and data were injured after using the policyholder's website. Without deciding whether there was actually indemnity coverage for the various claims asserted against the policyholder, the court held that the insurer had failed to carry its burden of demonstrating that each and every claim alleged by the aggrieved party fell outside the coverage provided by its policy. Policyholders faced with a third-party liability claim should look to this important, but sometimes overlooked, benefit of their policy to defend against costly litigation stemming from cyber-related crimes.

3. Coverage may hinge on whether the loss was "directly" related to the use of a computer.

Recent court decisions show that the availability of coverage will likely turn on the way in which the crime was committed, and more specifically, how "directly related" the use of a computer was related to policyholder's loss. Indeed, the concept of direct versus indirect loss is one of the most frequently litigated issues in cyber-related insurance coverage actions. Importantly for Ohio policyholders, the Sixth Circuit Court of Appeals has held that under Ohio law, language requiring that the policyholder's loss result "directly from" the fraudulent use of a computer is to be applied consistent with a proximate cause standard, and does not require that loss result "solely" or "immediately" from such use. *See Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, P.A.*, 691 F.3d 821, 831 (6th Cir. 2012). Notably, applying Michigan law to a case before it during the same year, the Sixth Circuit adopted a "direct-means-direct," or "immediate" causation standard to a similar claim. *See Tooling, Mfg. & Technologies. Ass'n v. Hartford Fire Ins. Co.*, 693 F.3d 665, 674 (6th Cir. 2012).

Cases from other jurisdictions, seemingly presenting similar fact patterns, have also reached different outcomes based upon differences in the underlying state law. For example, in both *Medidata Solutions, Inc. v. Federal Ins. Co.*, 2017 WL 3268529 (S.D. N.Y. July 21, 2017) and *American Tooling Ctr., Inc. v. Travelers Cas. and Sur. Co. of Am.*, 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017), the policyholder was victimized by criminals using spoofed emails to cause the policyholder's employees to wire funds to the criminals' bank accounts. In *Medidata*, the criminals utilized a series of spoofed emails and other communications to cause Medidata's employee to wire over $4 million to an overseas bank account believing that she was wiring the money pursuant to instructions from the company's management. Similarly, in *American Tooling*, the policyholder's employee received an email purporting to be from a vendor directing payments on outstanding invoices, totaling approximately $800,000, to the criminal's bank account.

Despite evaluating similar underlying facts, and applying similar policy language, the district courts reached opposite conclusions on the availability of coverage. In *Medidata*, the district court found that there was a sufficiently direct nexus between the fraudulent use of a computer and the policyholder's loss to provide coverage under Medidata's computer fraud and funds transfer fraud coverages. Distinguishing cases such as *Apache Corp. v. Great Am. Ins. Co.*, 662 Fed.Appx. 252 (5th Cir. 2016) and *Pestmaster Services., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 2014 WL 3844627 (C.D. Cal. July 17, 2014), *aff'd in part, vacated in part*, 656 Fed.Appx.332 (9th Cir. 2016), the court found that even though events occurred after the original fraudulent email to aid in the scam, the computer fraud was the direct cause of the loss because the "Medidata employees only initiated the transfer as a direct cause of the thief sending spoof emails posing as Medidata's president."

In *American Tooling*, the district court held that a vendor's spoofed emails, directing payment to the criminal's bank account, were not the "direct" cause of the policyholder's loss. Rather, intervening acts, such as the verification of production milestones, authorization of the transfers, and initiation of the transfers without verifying bank account information, "preclude[d] a finding of 'direct' loss 'directly caused' by the use of any computer." Both *Medidata* and *American Tooling* are on appeal to the Second Circuit and Sixth Circuit, respectively.

4. Coverage may depend on who caused your loss.

Coverage for cyber-related losses will frequently turn on who caused the policyholder's loss. For example, coverage may be precluded if the loss was caused by an employee, or by the unauthorized acts of an otherwise authorized user. For example, in *Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA*, 25 N.Y.3d 675 (2015), the policyholder suffered over $18 million in losses after it paid fraudulent claims submitted by authorized users of its online claims submission system. In holding that no coverage existed under the policyholder's computer fraud coverage, the court held that the policy insured only against "losses incurred from unauthorized access to Universal's computer system, and not to losses resulting from fraudulent content submitted to the computer system by authorized users." *Id.* At 680-81. Similarly, in *Pestmaster*, *supra* at *6, the court found that no coverage existed for theft by a policyholder's payroll administrator, because the administrator was authorized to withdraw funds from the corporation's bank account, even though he later used those funds for his own use.

5. Evaluate whether your policy covers this particular injury.

In the event the policyholder has coverage for the particular crime in question, it still must determine whether its policy covers the losses suffered by it or the third-party claimant. Disputes over what constitutes a covered loss, particularly in the CGL context, frequently center on whether the impacted property was "tangible property." For example, in *Eyeblaster*, the insurer argued that no coverage existed because the claimant alleged that he lost data when his computer was infected with spyware after using Eyeblaster's website. The court disagreed, finding that coverage potentially existed because the claimant also alleged that he lost use of his computer when the spyware caused it to freeze. The computer itself was "tangible property" that could be a covered loss under the policy at issue.

Similarly, in *Vonage Holdings Corp. v. Hartford Fire Ins. Co.*, 2012 WL 1067694, at *3 (D.N.J. Mar. 29, 2012), a federal district court held that a hacker's infiltration of Vonage's computer systems that enabled the hacker to transfer use of Vonage's telephone call routing servers to unauthorized persons constituted a "loss" that was arguably covered by Vonage's policy.

However, courts have also found that the loss of data alone, may not qualify as loss or damage to "tangible property." *See Liberty Corp. Capital Ltd. v. Sec. Safe Outlet, Inc.*, 937 F. Supp. 2d 891, 901 (E.D. Ky. 2013) (because customer email list "has no physical form or characteristics, it simply does not fall within the definition of 'tangible property.'"), *aff'd*, 577 Fed. Appx. 399 (6th Cir. 2014). *But see*, *Landmark Am. Ins. Co. v. Gulf Coast Analytical Labs., Inc.*, No., 2012 WL 1094761, at *4 (M.D. La. Mar. 30, 2012)(finding coverage for loss of electronic data).

The foregoing considerations are just a starting point for a policyholder faced with a potential or actual cybercrime loss. Policyholders are encouraged to work closely with their broker and risk managers when evaluating their risks and coverage needs, and to contact coverage counsel to assist with presenting claims to their insurer and responding to insurer inquiries.

Wes Lambert is a partner in Brouse McDowell's Litigation and Insurance Recovery Practice Groups. He represents corporate policyholders in maximizing insurance assets and recovering unpaid insurance proceeds. He has been a CMBA member since 2006. He can be reached at (330) 535-5711 or at wlambert@brouse.com.