BARNES & THORNBURG LLP

Gone Phishin': How Does Insurance Apply To Business Email Compromise Losses?

December 9, 2020 | Policyholder Protection,Insurance,Cyber Insurance,Data Breach

Carrie Marie Raver
Partner
Insurance Recovery and Counseling Group Co-Chair

Scott N. Godes
Partner
Data Security and Privacy Co-Chair, Insurance Recovery and Counseling Group Co-Chair

Suppose one of your business partners paid a multimillion dollar invoice to a fraudster, rather than to your business. Further suppose that the perpetrator had hacked your server, thereby enabling him to send out a fake invoice that appeared to have been sent by your business. Whose insurance policy covers the loss – the one issued to your business partner, or the one issued to your business?

This is not a far-fetched scenario. It is common enough to have a name – a "business email compromise," or "BEC." On April 6, 2020, the FBI reported that, "between January 2014 and October 2019, the Internet Crime Complaint Center received complaints totaling more than $2.1 billion in actual losses from BEC scams using two popular cloud-based email services." [1]

These scams continue to impact businesses, and are expected to worsen as cyber criminals take advantage of quarantines and thinned-out security teams resulting from COVID-19. [2] Allocation of responsibility – and insurance coverage – for these losses is an important issue for companies that cannot

RELATED PRACTICE AREAS

Data Security and Privacy
Insurance Recovery and Counseling

RELATED TOPICS

Insurance Coverage
Data Security

afford more negative pressure on their cash flow.

A BEC Scenario

Hackers can obtain access to a company's email server through various means, whether because an employee clicks on a phishing email, or because the hackers sneak in via a cloud provider. Once in, the hackers infiltrate a user's email account and set up rules that intercept messages from and to specified third parties. The hackers then send messages to a business partner (the buyer) that made purchases from the hacked company (the seller), including altered invoices or payment information. When the buyer receives a change in payment instruction from the hacked seller, it winds up paying the hackers instead of the seller.

When the seller goes to collect accounts receivable, it makes a demand on the buyer to pay its bill. The buyer protests that it has already done so. When the fraud is revealed, the seller points out that the buyer's naivete does not excuse its performance – it must pay the seller for goods or services received. The buyer replies that it has already paid, and that if the seller had better cybersecurity, the BEC would have been prevented.

Which Party Is Responsible for the Loss?

The law governing which party is liable in this scenario is developing. Some courts hold that the buyer must pay the seller because the buyer's payment to a hacker did not satisfy its contractual obligation to its counterparty. Other courts hold that the responsibility for the loss falls on the party most culpable in causing the loss. [3] Adding another level of complexity, the parties' contract or common law might require the seller to indemnify the buyer for its payment to the hackers caused by the seller's security lapse. There is little authority addressing the standard of care applicable to the seller's data security, and whether a buyer can recover from the seller based on negligence has yet to be definitively decided.

Does the Buyer's Insurance Cover the Loss?

The first place the buyer may look for coverage of its payment lost to the hackers is its own commercial crime insurance policy. Insurers say that a crime policy is first-party insurance that does not cover third-party claims. As such, insurers say that coverage applies to the insured’s out-of-pocket losses resulting from a covered peril – such as computer fraud and funds transfer fraud – rather than the insured’s liability to another party for the latter’s loss.

Crime insurers frequently deny coverage for BEC-related losses on grounds that the insured's loss was not the "direct" result of a use of a computer or a fraudulent instruction. Many crime policies require that an insured's loss result "directly" from a triggering act, with no intermediate steps between the hackers' infiltration of the seller's email system and the buyer's surrender of funds. Insurers contend that this requirement effectively limits coverage to narrow circumstances where a hacker accesses the insured's payment systems and steals money directly from the insured or issues fraudulent instructions directly to a financial institution. Well-reasoned decisions from the Second Circuit, Sixth Circuit, and Eleventh Circuit have rejected those arguments, and ruled in favor of coverage for BEC losses. [4]

Insurers have revised certain crime policy forms to try to limit coverage for

this kind of loss, either to exclude the loss entirely or add coverage for it back into the policy by endorsement for additional premium. Many insurers now sell "social engineering fraud" endorsements, charging a supplemental premium for the "new" coverage, often subject to lower limits. Social engineering fraud coverage typically applies where the policyholder is duped into wiring funds to a criminal after receiving fraudulent emails, as in the scenario above. But it should be noted that computer fraud coverage still might apply to BEC losses if the emails are the result of a hacker getting access to the policyholder's system.

Does the Seller's Insurance Cover Liability to the Buyer?

If the seller is legally responsible to the buyer for damages – that is, liable to pay the amount that the buyer paid the hackers – the seller's cyber insurance policy with network security liability coverage might apply to the buyer's claim against the seller to recover its unwitting payment to the hackers. Cyber insurance policy terms vary, but network security coverage typically applies when there has been a breach of cybersecurity, a demand for payment, and resulting damages.

The scenario above likely meets each of these requirements. The unauthorized access to and use of the buyer's system should meet the definition of "network security" in many cyber insurance policies. The buyer's response to the seller upon learning it has been defrauded (i.e., that it paid for the goods or services it received and will not do so twice) might satisfy a policy requirement of a formal, written demand for payment.

Amounts the seller has to pay the buyer to compensate the buyer for funds it paid the hacker should constitute "damages" or "loss" resulting from the seller's legal liability to its customer. In short, most sellers' network security liability insurance policies should cover this liability.

Yet insurers can be counted upon to disagree. They likely will argue that various policy exclusions apply, or that the loss falls within exceptions embedded in the definition of covered "damages" or "loss." They may also take the position that the loss involves nothing more than a contractual dispute which, in their view, insurance policies do not cover. In the case of a cyberattack in which the buyer pays a fraudster instead of the seller, the buyer might claim that the seller is liable for the amount that the buyer paid to the fraudster. A carrier might assert that the claim is not for "damages," or otherwise is excluded, because it is an amount that the buyer owes the seller anyway.

An overlapping type of coverage for the seller is found in a newly developed product in the insurance market: "invoice manipulation fraud" coverage. This new coverage is available from some carriers by endorsement to cyber insurance or crime insurance policies. It applies when the policyholder's invoices were manipulated, and the policyholder is not paid because the buyer paid a fraudster instead of the proper party. However, it may be subject to a sublimit of coverage.

Takeaways

To ensure your company has protection against BECs, consider the following best practices when renewing insurance programs:

1. Check whether the insurance program includes coverage for social

engineering fraud, invoice manipulation, and network security coverage. Does your company have this coverage in its policy forms? Is the insurer offering this coverage by endorsement for an additional premium?
2. Check the policy limits that would apply to those coverages. Binder letters might not disclose a sublimit on certain insuring agreements.
3. Consider how excess coverage will apply. If the primary policy has lower coverage limits for BEC losses, policyholders should explore whether excess policies will "drop down" to attach at the level of any sublimits, to avoid coverage gaps.

This article was originally published in the 2020 edition of Corporate Policyholder Magazine.

---

[1] *FBI, Cyber Criminals Conduct Business Email Compromise Through Exploitation Of Cloud-Based Email Services, Costing Us Businesses More Than $2 Billion, Federal Bureau of Investigation Internet Crime Complaint Center, https://www.ic3.gov/media/2020/200406.aspx (Apr. 21, 2020).*

[2] *FBI National Press Office, FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic, Federal Bureau of Investigations, https://www.fbi.gov/news/pressrel/press-releases /fbi-anticipates-rise-in-business-email-compromiseschemes-related-to-the-covid-19-pandemic (Apr. 21, 2020).*

[3] *See, e.g., Arrow Truck Sales, Inc. v. Top Quality Truck & Equip., Inc., 2015 U.S. Dist. LEXIS 108823, *15-16 (M.D. Fla. Aug. 18, 2015).*

[4] *Medidata Sols., Inc. v. Fed. Ins. Co., 268 F. Supp. 3d 471 (S.D.N.Y. 2017); Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455 (6th Cir. 2018); Principle Sols. Grp., LLC v. Ironshore Indem., Inc., 944 F.3d 886 (11th Cir. 2019). The authors of this article were coverage counsel for the last case.*