ROCHESTER BUSINESS JOURNAL
Part of the BRIDGETOWER MEDIA network
OCTOBER 10, 2022

# Important considerations when evaluating cyber insurance coverage

■ Ryan Lema


*Lema*

DATA BREACHES AND CYBERCRIMES have become all too common. Companies large and small now find themselves the target of cyberattacks in the form of ransomware, phishing emails and social engineering attacks. The resulting data breaches can result in business interruption and downtime, loss of confidential information, and the potential for significant costs and damages.

Cyber liability insurance policies provide policyholders with several coverages to protect businesses from first-party losses and third-party claims arising from data breaches and other cybersecurity issues.

## Types of cyber insurance coverages

Generally, cyber insurance policies will protect your company from cyber risks with several distinct coverages, which may include the following:

- **Network security** – typically covers your business in the event of a breach of network security, such as a data breach, malware infection, ransomware or other electronic compromise.
- **Privacy liability** – will provide coverage for third-party losses arising out of a security breach. For example, this type of coverage would defend and indemnify in connection with consumer litigation over a data breach, or cover the various expenses, fines and penalties incurred in connection with an investigation by government regulators or law enforcement.
- **Errors and omissions (E&O)** – will afford protection where a cybersecurity incident prevents your company from meeting its obligations. E&O coverage would respond to third-party claims in such an event.

Cyber insurance policies may also include additional optional coverages, each with its own specific sub-limits:

- **Social engineering** – covering businesses for fund transfers initiated by fraud, such as when an employee is tricked into sending money to a third party by fraudulent wire instructions.
- **Reputational harm** – covering business losses due to reputational damage for a specific time period following a publicized cyber event, such as a data breach.
- **Device damage** – covering the replacement cost of computers, phones or other hardware rendered unusable by a malware attack.

While most cyber insurance policies will contain some combination of the above coverages, there will be differences between policies (particularly

ROCHESTER BUSINESS JOURNAL

*In reviewing the coverage afforded under a cyber insurance policy, policyholders should be mindful of the different coverages provided and the different limits that may be applicable to each type of coverage.*

when purchasing a stand-alone cyber insurance policy or adding cyber coverages to a package policy). As part of your company's overall risk management strategy, you should review the cyber coverages that you have in place and the limits applicable to each type of coverage in relation to your company's operations and risk profile.

## Recent cases highlight the important distinction between coverage for hacking events and social engineering attacks

In reviewing the coverage afforded under a cyber insurance policy, policyholders should be mindful of the different coverages provided and the different limits that may be applicable to each type of coverage. One ongoing case in the Northern District of Illinois[1] highlights the important distinctions between different cyber coverages — and the need to carefully review cyber coverages with your counsel and insurance professionals.

In this case, the Illinois Department of Insurance is seeking coverage for losses caused by a fraudulent email sent to an employee in the Department's Office of the Special Deputy Receiver ("OSD"). The fraudulent emailer, posing as OSD's chief financial officer, convinced an employee to transfer nearly $7 million to overseas accounts.

OSD filed suit against two of its insurance carriers seeking coverage under the computer fraud provisions of OSD's cyber insurance policies.

The insurance companies have moved to dismiss OSD's claims, noting that the policies contain separate insuring agreements for "computer fraud" and "social engineering." "Social Engineering" coverage responds to fraudulent inducement by means of misrepresentations by a third party, whether by email or other electronic means. This coverage for social engineering attacks is distinct from coverage for computer fraud, which responds to losses due to computer crimes — the intentional, fraudulent or unauthorized input, destruction or modification of electronic data or computer instructions by a third party (i.e., computer hacking).

The distinction between which of the policies' coverages might apply is not an academic exercise: in OSD's case, its two policies afforded only $500,000 in combined coverage for social engineering losses, whereas limits for computer fraud coverage total over $5 million between the two policies. This case highlights the important distinctions between cyber coverages and the need for policyholders to understand and consider the limits of insurance that they procure to protect against each type of risk.

*Ryan A. Lema is a partner with Phillips Lytle LLP and member of the firm's Insurance Coverage Practice Team. His experience with insurance coverage matters includes litigating complex coverage disputes for insureds, litigating insurance procurement and indemnification disputes, working with primary and excess insurance carriers to defend the interests of insureds, and monitoring defense claims where the claim exceeds insurance coverage. He can be reached at (716) 504-5790 or rlema@phillipslytle.com.*

[1] Off. of Special Deputy Receiver ex rel. Severinghaus v. Hartford Fire Ins. Co., No. 22-cv-03709 (N.D. Ill. filed July 18, 2022).