The Computer & Internet Lawyer

Volume 37 ▲ Number 3 ▲ MARCH 2020

Ronald L. Johnston, Arnold & Porter, LLP, Editor-in-Chief

Issues to Consider When Evaluating Cyber Coverage in Light of the CCPA and Other State Privacy Laws

By Michelle A. Reed, Natasha G. Kohne, Diana E. Schaffner, and Rehan M. Safiullah

With the expansion of privacy legislation – from the General Data Protection Regulation ("GDPR") in Europe to the California Consumer Privacy Act ("CCPA") in the United States – cyber liability insurance is taking on increased importance. This article discusses key issues companies should consider as they review their cyber coverage in light of changing legislation and increased litigation risks. Companies should act now to ensure they have sufficient cyber coverage in place now that the CCPA has gone into effect.

Michelle A. Reed (*mreed@akingump.com*), a partner in the Dallas office of Akin Gump Strauss Hauer & Feld LLP, is co-leader of the firm's cybersecurity, privacy, and data protection practice. **Natasha G. Kohne** (*nkohne@akingump.com*), a partner in the firm's San Francisco office, is co-leader of the firm's cybersecurity, privacy, and data protection practice. **Diana E. Schaffner** (*dschaffner@akingump.com*), counsel in the firm's San Francisco office, advises clients on privacy- and cybersecurity-related litigation, investigations, and enforcement actions. **Rehan M. Safiullah** is a former senior counsel in the firm's Houston office.

Covering costs related to data breach response and recovery and data breach- and privacy-related enforcement actions and litigation presents challenges. Worldwide, as of April 2019, the average total cost of a data breach was $3.92 million.[1] The average total cost of a data breach in the United States was $8.19 million.[2] The costs of enforcement actions can be similarly significant in terms of monetary penalties and secondary costs. Without adequate coverage, these costs can have long-term effects on a business.

Principal Coverages

Cyber policies are now a common part of most companies' insurance portfolios. The policies generally cover five principal areas:

1. Costs to manage and respond to a cyber-incident;
2. Costs stemming from network interruption;
3. Costs for security and privacy liability;
4. Costs relating to extortion; and
5. Costs for media liability or reputational harm.

Whether insurers cover all of these areas or all costs within different areas varies from policy to policy. Most policies offer first-party and third-party coverage.

First-party coverage applies to losses that are directly sustained by the insured party, such as damage to a company's own electronic data files.

Third-party coverage applies to claims by others against the insured company, such as claims by people who were injured by the insured company's actions (or inactions).

With the increase in state privacy legislation, particularly the CCPA, many insurance companies are working with clients to also cover certain "compliance" costs arising out of a violation of a privacy-related legal obligation where no underlying cyber incident has occurred. Insurers and insureds alike are also working to understand how the CCPA's private right of action fits within existing third-party liability coverage and whether and how they may need to expand such coverage. We provide below a few points of guidance for companies to consider as they engage in similar discussions with their brokers and insurers.

Potential Gaps in Cyber Coverage

Companies should consider the following potential gaps, among others, in cyber coverage as they evaluate their policies in the lead-up to the CCPA and in light of other state privacy laws.

"Compliance" Coverage

Not all policies clearly cover regulatory fines that federal or state regulators may impose for a company's violation of a privacy statute where no underlying cyber incident occurred. Instead, some policies link reimbursement to the existence of a breach and its documentation. With the adoption of laws like the GDPR and the CCPA, some insurance companies are also offering cyber coverage that includes a "compliance" element.

This is important because regulatory fines present significant potential costs. Under the CCPA, state regulatory fines range between $2,500 and $7,500 (intentional) per violation. A breach exposing 10,000 records could, if each record is considered a separate violation, lead to fines of tens of millions of dollars.

Compliance coverage provides protection for regulatory fines where there is no underlying cyber incident. Some insurance companies also offer services to help incentivize compliance, like regulatory readiness assessments.[3] Compliance coverage may apply, for example, where a regulator fines a company for failing to timely or properly respond to a consumer (or data subject) request for information. Many companies with a European presence sought similar coverage before the GDPR took effect in May 2018. Companies required to comply with the CCPA should consider doing the same.

Coverage for Litigation Costs

Not all policies cover data breach- and privacy-related litigation costs, and others limit the type of litigation costs covered. The CCPA includes a private right of action that many believe will spawn a new wave of privacy class actions. The CCPA provides consumers a private right of action in the event their personal information is affected by a data breach and certain other conditions are met. Consumers may seek the greater of either actual damages or statutory damages ranging from $100 to $750 per consumer per incident. Defense costs could similarly increase as companies defend against shareholder lawsuits and other related litigation. A cyber policy that covers litigation defense helps a company prepare for and mitigate these costs.

Companies should consider policies that include robust third-party liability coverage. They should also write into their policies their outside counsel of choice to ensure there is no dispute down the line as to their ability to hire trusted counsel.

Coverage for Intentional Acts of Employees

Some cyber policies exclude coverage for intentional acts by the insured's employees. It is important to understand how this limitation may affect coverage for costs related to the access and disclosure of information by an employee not authorized to access such information. Some new state laws expand the definition of a breach to include "access," not just acquisition, in certain circumstances. For example, the CCPA may be interpreted as expanding the definition of "breach" to include unauthorized access and disclosure. The New York Stop Hacks and Improve Electronic Data Security ("SHIELD") Act similarly expands the definition of "breach of the security of the system" to include unauthorized access.

Coverage for Cyber Fraud

Keep in mind that fraud, even if cyber-related, may fall under a separate crime policy. Companies should think through how their cyber and crime policies may interact with regard to recovery of costs related to, for example, fraudulent consumer information requests. Recent reports suggest that companies subject to the GDPR have faced an onslaught of fraudulent data subject requests, which are akin to consumer information requests under the CCPA.[4] Companies may want to

prepare for a similar situation when the CCPA goes into effect.

Follow Policy Requirements to Ensure Coverage

Beyond potential gaps in coverage, companies should also carefully note additional obligations that they may need to comply with to ensure coverage. Companies should work these obligations into their incident response plans, including by assigning responsibility for the tasks to specific members of their incident response teams. These obligations may include notification obligations or use of insurer-mandated service providers (for example, a particular cybersecurity forensic firm). Companies should write into their policies their outside counsel of choice to ensure high-quality representation by firms that are familiar with and trusted by their company.

Risk Of Insurance Denial of Coverage For Certain Types of Incidents

In the midst of these changes, a few pending cases could lead to troublesome precedent in terms of easing insurance companies' ability to avoid payment of certain cyber-related claims. The most significant of these cases involves a claim Mondelez (a multi-national company with brands such as Oreo and Ritz Crackers) filed under its property policy related to costs incurred as a result of the NotPetya ransomware attack in 2017. After U.S. government authorities attributed the NotPetya attack to a foreign state actor, Mondelez's insurer used that attribution to assert that Mondelez's claim was barred under a war exclusion clause. The parties are now locked in litigation regarding the applicability of the exclusion.

Other potential cybersecurity insurance risk areas include:

1. Lack of coverage for accidental errors and omissions (as opposed to attacks and unauthorized activity);

2. In cases where there was significant business interruption, some insurers are limiting claims to losses incurred during actual network interruption, not the entire period of business interruption;

3. Where the data breach occurs with a third-party contractor or outsourced service provider, some insurance policies do not cover such breaches; and

4. Unclear allocation between cybersecurity policy and crime/fraud policy in the case of fraudulent wire transfers originating from business email compromise.

Companies should monitor this and other cyber insurance disputes to ensure they update their policies as necessary.

Conclusion

With the CCPA now in effect, companies that have not done so already should reach out to their outside counsel and brokers to understand what coverage they have, what coverage they think they need and the cost/benefit to buying additional cyber coverage. The following are points companies should consider as they reevaluate their cyber insurance coverage in light of the CCPA and other state privacy laws:

- Prepare, or ask your broker to prepare, an overview of your current cyber coverage, including whether it includes "compliance" coverage, permits recovery of costs related to an investigation where no underlying cyber incident is discovered (even if no official action is taken by a regulator), covers unauthorized access by employees, includes litigation costs and similar key issues.

- Ensure you obtain expanded litigation coverage, if you intend to, by January 1, 2020. The CCPA's private right of action is apparently effective as of that date, although public enforcement of the CCPA will not begin until at least July 1, 2020.

- Write your outside counsel of choice into your cyber policy. Many insurance companies still provide companies the option of doing so and it can facilitate cost recovery to ensure this is done before an event occurs.

- Update your incident response plans to incorporate key obligations in your cyber policy to ensure you meet all prerequisites for recovery. Incorporate any mandated service providers into your incident response team, as appropriate. Review the California Attorney General Office's regulations once released to see if they suggest you may need additional coverage.

- Monitor developments related to the CCPA, particularly the private right of action, and reevaluate your insurance coverage at the end of 2020 to determine if you should adjust your coverage.

- Assign someone on your team, or request outside counsel, to monitor federal and state privacy and cybersecurity developments and schedule regular (perhaps quarterly) updates to ensure your team understands any developing requirements.

Notes

1. IBM Security, Cost of a Data Breach Report (April 2019), p. 3, *available at https://www.ibm.com/security/data-breach*.
2. Id.
3. *See, e.g.*, Insurance Journal, AXA XL Adds Cybersecurity Services to Cyber Insurance Program (Nov. 30, 2018), *available at https://www.insurancejournal.com/news/national/2018/11/30/510695.htm*.
4. *See* The Register, Talk about unintended consequences: GDPR is an identity thief's dream ticket to Europeans' data (Aug. 9, 2019), *available at https://www.theregister.co.uk/2019/08/09/gdpr_identity_thief/*.