wiley

ARTICLE

The Problem With Breachless Cyberinsurance Claims

Law360
October 24, 2016

The recent headlines regarding Johnson & Johnson's disclosure "that a person could potentially gain unauthorized access to [a certain insulin] pump through its unencrypted radio frequency communication system," described by the company as a "cybersecurity issue," reflect the fact that companies are identifying security concerns involving products in the marketplace even before a hacking incident has taken place. SeeAnimas customer letter (Oct. 4, 2016), here. These types of incidents are increasingly leading to claims and regulatory investigations focused on cyber security issues even in the absence of any data breach or computer security breach.

The availability of insurance coverage under cyberpolicies for these "breachless" claims will hinge on the specific language of the policy at issue, as well as the unique facts at play. In some instances, cyberpolicies will not afford coverage for the costs of addressing the issue because the insured cannot show that the policy's trigger of coverage—an actual or reasonably suspected breach—is present. Insurers and insureds will need to pay careful attention to the specific facts and policy language at issue when analyzing the potential of coverage.

Background

In the aftermath of a data breach, a company may quickly face claims on multiple fronts, including from consumers, businesses, and regulatory authorities. A cyberbreach in many circumstances will involve harm to persons or organizations whose sensitive information is in fact compromised and misused. Those claims may fall within the general scope of coverage afforded by cyberinsurance policies

Authors

Mary E. Borja
Partner
202.719.4252
mborja@wiley.law

Practice Areas

Cyber Insurance
Insurance
Privacy, Cyber & Data Governance

because one of the necessary predicates to trigger coverage under many cyberinsurance policies—unauthorized access to sensitive information through the failure of computer security—is present. See, e.g., *P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.*, No. 15-cv-1322 (SMM), (D. Ariz. May 31, 2016).[1]

In addition to these "breach" claims, however, companies and other organizations are increasingly facing "breachless" claims, such as those involving unexploited vulnerabilities. These claims, while less common, often involve a different set of issues for the purposes of evaluating potential insurance coverage. Insurers will therefore need to evaluate these claims carefully, and insureds should examine their risk management strategies, such as through insurance and contractual indemnification, to mitigate potential exposure for liability.

To illustrate, a number of private putative class actions have been filed alleging security defects in certain products. See, e.g., *Cahen v. Toyota Motor Corp.*, 3:15-cv-01104-WHO (N.D. Cal.) (alleging that defendant automobile manufacturers "sold or leased vehicles that are susceptible to computer hacking and are therefore unsafe"); *Ross v. St. Jude Medical Inc.*, No. 2:16-cv-06465-DMG (C.D. Cal.) (seeking damages and alleging that a "vulnerable communication channel in an implanted ... device ... could result in a major privacy breach"). These claims do not allege that a vulnerability has been exploited, but instead complain about potential vulnerabilities and allege harm from the existence of a potential for a breach. Plaintiffs commonly allege that they did not obtain the full benefit of their bargain because these vulnerabilities were neither known nor disclosed to them at the time they purchased the products.

In addition to claims by private litigants, companies may also face claims, inquiries, or investigations from regulatory authorities even in the absence of a breach. See, e.g., *In re Dwolla, Inc.*, No. 2016-CFPB-0007 (Doc. 1, filed March 2, 2016) (consent order between company and CFPB entered into regarding alleged misrepresentations with regard to a company's data security practices despite there being no evidence of that consumers actually suffered tangible harm); see also Joe Carlson, *FDA joins investigation into security of St. Jude medical devices*, Star Tribune (Aug. 26, 2016) (available at http://www.startribune.com/st-jude-medical-sharply-criticizes-short-seller-s-attack-on-its-cybersecurity/391437581/) (discussing security of certain medical devices and noting that the U.S. Food and Drug Administration "confirmed that it has joined an investigation of claims that the devices can be hacked remotely"). These matters arise from a number of different sources and involve a variety of regulatory agencies.

Coverage Implications

These "breachless" claims present important questions for cyber insurers regarding the scope of coverage afforded under their policies. Given the wide variety of forms in the marketplace, this determination will often require careful analysis of the specific language of each policy to determine whether and to what extent coverage may respond.

As with any insurance policy, a policyholder bears the initial burden of proving that a coverage grant in its insurance policy has been triggered. See, e.g., *Consolidated Edison Co. of New York, Inc. v. Allstate Ins. Co.*, 774 N.E.2d 687, 690 (N.Y. 2002). Cyberpolicies are virtually always written on a claims-made basis, and they

often include a threshold requirement of the existence of a breach (or reasonably suspected breach) that is first discovered during the policy period. If the policy trigger includes the actual or reasonably suspected breach, a cyberpolicy may simply not respond to the "breachless" claim.[2]

In addition to third-party liability coverage, cyberpolicies often afford first-party coverage for the insured's own costs of investigating and responding to a breach. The trigger of coverage under the first party coverage part in many cyber policies is the existence of a known or reasonably suspected breach of a company's computer network (provided it is first discovered during the applicable policy period). This coverage is not written to cover generalized concerns regarding data security. If it were, insurers would face an endless flow of claims given the needs of many insureds to work continuously to improve the security of their systems. Instead, it is triggered only when the insured discovers indicia that sensitive data was compromised. The availability and extent of coverage may in some respects mirror the triggers for reporting and notice obligations under state breach notification laws. See, e.g., Cal. Civ. Code § 1798.82(a) (requiring notification to persons whose "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person"). In this way, first-party cybercoverage may be analogous to a commercial crime policy; while a commercial crime policy may afford certain coverage for a first-party loss after a crime has taken place, it typically does not cover the expenses of investigating potential holes in a company's security procedures that may enable crime to happen in the first instance. Likewise, a cyber policy may be triggered for first-party loss in the aftermath of an actual breach of the insured's data or computer system, but it does not afford coverage for the costs to simply assess an insured's systems or detect potential ways that a vulnerability might be exploited. In sum, in the absence of an actual breach event, and where there is no likelihood that sensitive information was actually or reasonably believed to have been compromised, first-party coverage seems unlikely to be available under a cyberpolicy.

Third-party liability coverages under cyberpolicies often are written to apply only to claims involving the same events that trigger coverage in the first-party context—i.e., when there has been a data breach event (including a reasonably suspected compromise of data). Were it otherwise, these policies might be swept into coverage disputes when there were allegations of inadequate data security, even if the focus of those disputes was clearly on other, uncovered events.[3] Cyberpolicies thus often differ from other claims-made errors and omissions or directors and officers liability policies triggered simply by a "Claim" for a "Wrongful Act" in that, as noted above, there is an additional requirement for the existence of a breach event.

Conclusion

While cyberinsurance policy forms vary widely, the existence of an actual or reasonably suspected breach is fundamental to many cyber insurance policies currently in the marketplace. The "breach" is an essential element to trigger coverage. As claims and investigations that do not involve an actual or even reasonably suspected breach are becoming increasingly common, insurers and insureds must carefully examine the specific facts and policy language of a given matter to determine the existence of coverage.

[1] An appeal has been filed in the *P.F. Chang's* case. *See* Case No. 16-16141 (9th Cir.).

[2] Claims involving products may also give rise to other dispositive coverage issues. For example, many cyberpolicies respond only to incidents affecting specified computer systems. For claims involving the security of products or systems that do not fall within those networks, there may be no coverage for that independent reason.

[3] For example, a former employee asserting a claim for wrongful termination for "blowing the whistle" on potential security vulnerabilities would involve allegations of improper data security, but it would not trigger coverage under a cyberpolicy.