Cybersecurity Policy Report
Strategic Perspectives

Wolters Kluwer

August 4, 2021

Cyber Insurance 101

By Emily Garrison and Sara Brundage of Honigman LLP

As cybersecurity incidents increase in frequency and scope, cyber insurance policies are an important tool for companies to mitigate loss from such incidents. Recent surveys of small and medium businesses reveal, however, that many respondents do not carry cyber insurance.[1] And for those that do, the cost of such coverage is rising. For companies considering purchasing or renewing a cyber policy in light of new or increasing risk, this article provides a brief primer on the types of coverages that cyber policies offer, potential add-ons to coverage, common conditions and exclusions, and other cyber insurance-related questions.

What does a cyber policy cover?

Cyber policies generally cover two types of risks: (1) first party coverage for the policyholder's own losses or damages incurred in responding to a data breach or other cyber incident; and (2) third party liability coverage provides protection in the event of claims against the policyholder because of a data breach or cyber incident, such as privacy lawsuits by consumers. Policies and coverage terms are highly variable and policies should be reviewed in their entirety. Nevertheless, some common coverages (or enhancements) that may be available include:

First Party Coverages:

- *Incident response*: the most standard coverage in a cyber policy is for the costs of investigating, responding to, and terminating an actual or suspected data breach or other cyber incident. This coverage often includes the legal costs associated with determining whether a policyholder is required to give notice of a breach to a government agency or persons / entities impacted by the breach.
- *Forensic fees*: this coverage includes the costs to investigate the cause of the data breach or other cyber incident and to identify the individual or entities responsible for the breach.
- *Notification, credit and identity monitoring*: this coverage includes the costs of notifying third parties, including vendors, customers or government entities about the loss. The costs of call center services to address inquiries about the breach, as well as credit monitoring services and identity theft protection for those impacted by the data breach may also be covered.
- *Data recovery*: if software or electronic data is damaged, altered, corrupted, or destroyed following a breach, this coverage includes the costs to determine the scope and cause of such loss, and the costs to restore control over or to replace, restore or recollect data.

- *Business interruption*: generally provides coverage for income loss resulting from a cyber incident, for example if production is halted after a malware attack. It may also include coverage for costs associated with continuing to run the policyholder's business, including payroll expenses, as well expenditures in excess of normal operating costs that are required to keep the business going and reduce the impact of income loss. Contingent business interruption coverage may also be available in the event of losses resulting from damage to a shared computer system or the computer system of a service provider or supplier.
- *Cyber extortion*: provides coverage for ransomware and other cyber extortion, including ransom payments and the costs of hiring an expert to respond to a threat or demand. Coverage may also include amounts paid to obtain cryptocurrency that is demanded by a cyber-criminal.
- *Cyber crime (other):* in addition to cyber extortions, policies may cover losses due to phishing attacks, fraudulent instructions, business email compromise / social engineering or invoice manipulation fraud.[2]
- *Reputational damage*: covers certain costs for public relations, media purchasing or other costs to mitigate harm to a policyholder's reputation after a data breach or other cyber incident.

Third Party Coverages:

- *Security and Privacy Liability*: protects the policyholder against losses, including defense costs, settlement costs and/or judgments incurred as a result of claims brought by third parties in connection what a data breach or cyber incident, including claims for the transmission of malicious code to a third parties' computer or claims for failure to protect private or protected information. Also may provide coverage for actual or alleged violations of federal, state, local or foreign law or regulation regarding the collection, maintenance, protection, use or disclosure of private or protected information, and/or violation of any company policy relating to private or protected information.
- *Multimedia / Media Communications Liability*: protects the policyholder against losses, including defense costs, settlement costs and/or judgments incurred in connection with claims brought by third parties for defamation / libel / slander / product disparagement and related torts, invasion, infringement or interference with an individual's right of privacy, plagiarism, piracy, copyright and trademark infringement, and similar claims.
- *Regulatory Defense and Penalties*: provides coverage for defense expenses, fines and penalties associated with an investigation or administrative or civil proceeding brought by a regulatory agency in connection with a data breach or cyber incident.
- *PCI DSS Liability*: covers amounts policyholder is obligated to pay as assessments, fines, or penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) or payment card company rules, and related defense costs.
- *TCPA Defense*: some policies may offer coverage for defense costs associated with defending claims brought under the Telephone Consumer Protection Act.

Are there conditions or exclusions that limit coverage?

Policyholders that have purchased a cyber policy and experience a cyber incident are often surprised by the notice, consent and approved counsel / vendor provisions of their policies. Reviewing these provisions in advance and negotiating more favorable language (if possible) could eliminate or reduce this surprise:

- *Notice*: Cyber policies may have stringent notice provisions, including requiring notice within a certain number days after a breach. Notice provisions may also be linked to discovery or knowledge by certain individuals within a company, for example reporting is not required until the CEO, CFO or General Counsel becomes aware of a cyber incident or claim. Policies may also be written such that coverage will not be provided for amounts incurred prior to notice being given, unless the amounts were necessary to stop a cyber incident.
- *Consent*: Cyber policies also may have strict consent provisions, requiring prior written consent from the insurer to incur any responsive costs, including attorneys fees or costs of incident response vendors. Policies that provide coverage for ransom payments may also require the insurers' consent prior to making such a payment.
- *Approved counsel / vendors*: In addition to notice and consent provisions, cyber policies often include provisions requiring that policyholders use defense counsel or third-party incident response vendors from a pre-approved list provided by the insurer. Policyholders may be able to add their preferred counsel to such lists during policy negotiations, or at minimum include language that gives them the ability to share in the decision to choose counsel or service providers. Some policy forms have provisions allowing policyholders to choose their own counsel or service providers, but in those cases the costs of policyholder-selected vendors erode the limits of liability (whereas costs for the insurers' pre-approved vendors *do not* erode the limits).

With respect to exclusions, the variability of cyber insurance policies is particularly evident in their exclusions. For example, while one policy may provide coverage for TCPA defense costs as noted above, another policy may exclude coverage for TCPA and related claims. The same is true for cyber extortion or regulatory penalties, which may be affirmatively covered in some policies, but expressly excluded in others. It is thus important in all circumstances to carefully study policy exclusions before a policy is purchased. Although little case law exists regarding cyber policy exclusions, two exclusions that have been raised in litigation and thus are worth noting are:

- *Failure to Maintain Minimum Security Standards*: these exclusions provide that there is no coverage if the insured fails to maintain certain minimum security standards, including standards that are identified in a cyber policy application. For example, in *Columbia Casualty Company v. Cottage Health System*, the insurer filed a complaint seeking a ruling that it was not liable for losses arising out of a data breach pursuant to an exclusion for losses based upon, directly or indirectly arising out of, or in any way involving "[a]ny failure of an Insured to continuously implement the procedures and risk controls identified in the Insured's application."[3] Although this case was ultimately dismissed on procedural grounds based on an alternative dispute resolution provision of the policy, the complaint alone provides a cautionary tale for policyholders regarding policy exclusions.

- *Contractual Liability Exclusion*: these exclusions generally provide that there is no coverage for liability assumed by the policyholder under a contract agreement. There may be carveouts to the exclusion, including for liability that the policyholder would have incurred in the absence of such agreement. In *F. Chang's China Bistro, Inc. v. Federal Insurance Company*, hackers obtained and posted on the internet credit card information for tens of thousands of P.F. Chang customers. As a result, P.F. Chang was assessed approximately $2 million in charges by Bank of America Merchant Services ("BAMS"), which processed credit card payments made by the restaurant's customers.[4] The court held that these losses were not covered because P.F. Chang's liability arose out of its agreement to indemnify BAMS, and the cyber policy contained a contractual liability exclusion and an exclusion for "any costs or expenses incurred to perform any obligation assumed by, on behalf of, or with the consent of any Insured". Policyholders should review their policies and contracts to determine the scope and possible extent of such exclusions, if any.

Is Tech E&O insurance different from Cyber Insurance?

Technology errors & omissions ("Tech E&O") insurance is a type of professional liability policy. Although it covers different risks than a cyber policy, a Tech E&O policy can be a critical component of a technology company's arsenal. Tech E&O policies are designed to cover providers of technology products and services. Simply put, the coverage protects a technology company from claims by its customers in the event its tech-based services fail. This is different from cyber insurance, which responds to losses following data breach or cyber incident (as opposed to the failure of a service/product).

The interplay of the two coverages can be complicated. Consider, for example, which policy responds when a technology company's product fails and a consumer's personal information is exposed? Depending on the types of claims that arise out of the incident, both the Tech E&O policy (product failure) and the cyber policy (data breach) could be triggered. Because of the potentially overlapping issues, cyber policies and Tech E&O policies are often "bundled" together to eliminate potential gaps or overlapping coverages, and to ensure that the policies work together in harmony. Technology companies that are purchasing or renewing cyber coverage should consider whether they also have (or need) a Tech E&O policy, and how the policies work together to respond to potential risks or exposures.

What about traditional property and liability policies?

Policyholders have had success in many instances filling the cyber gap through traditional property or general liability policies.[5] Such claims, however, can be fraught with obstacles. Home Depot, for example, just filed a lawsuit this month against its commercial general liability insurers seeking $50 million in coverage for a 2014 data breach.[6] For over two and a half years, Mondelez International and Zurich have been litigating coverage for losses incurred by Mondelez in connection with the "NotPetya" cyberattack under an "all-risks" property insurance policy, including whether the "war" exclusion in the policy precludes coverage.[7]

For many policyholders, drawn out disputes and lawsuits are not financially viable. In addition, insurers – including AIG and Lloyd's of London – have stated that they are taking action to eliminate so-called "silent cyber" exposures by issuing policies that either affirmatively exclude or provide coverage for cyber risks.[8] These developments may encourage a policyholder to purchase a separate cyber policy, but in the event of a cyber incident, policyholders should nevertheless carefully study all policies to determine if coverage is available and to ensure compliance with applicable notice provisions.

Conclusion

There are many business reasons for why a company may or may not purchase insurance. With cyber insurance in particular, its relative novelty and the lack of standard form policies, coupled with time-consuming applications and incomplete or even incorrect information in the market about cyber insurance can make some reticent to take the leap and purchase a policy. Appropriately tailored and narrowed cyber insurance program can, however, provide valuable coverage to mitigate against the myriad of cyber risks that companies face on a day to day basis. Companies that are potentially at risk for data breaches, ransomware attacks or other cyber incidents should comprehensively review their insurance programs and reach out to an experienced broker or insurance coverage lawyer with questions.

Endnotes

1 See, e.g., https://cyberscout.com/en/press-releases/majority-of-us-small-and-medium-sized-businesses-do-not-have-cyber-insurance and https://www.prnewswire.com/news-releases/selective-survey-finds-majority-of-small-businesses-lack-cyber-insurance-coverage-301247484.html

2 These types of coverage may also be endorsed to a commercial crime policy. It is always important to review all available coverages in the event of a cyber incident or attack.

3 *See Columbia Casualty Company v. Cottage Health System,* Case No. 2:15-cv-03432 (C.D. Cal.) (complaint filed May 7, 2015).

4 *P.F. Chang's China Bistro, Inc. v. Federal Insurance Company,* 2016 WL 3055111 (D.Ariz. May 31, 2016).

5 *See, e.g., G&G Oil Co. of Indiana, Inc. v. Continental Western Insurance Co.,* 2021 WL 1034982 (Ind. March 18, 2021) (bitcoin ransom payment potentially covered under crime policy); *The Travelers Insurance Company of America v. Portal Healthcare Solutions,* 35 F. Supp. 3d 765 (E.D. Va. 2014), aff'd by 644 Fed.Appx. 245 (4th Cir. 2016) (insurer ordered to defend insured in data breach lawsuit under commercial general liability policy); *West Bend Mutual Insurance Company v. Krishna Schaumburg Tan, Inc.,* 2020 IL App (1st) 191834, 2020 WL 1330494 (Ill.App. 2020) (general liability insurer had duty to defend lawsuit brought under Illinois Biometric Information Privacy Act) (currently on appeal).

6 *The Home Depot, Inc., et al. v. Steadfast Ins. Co., et al.,* Case No. 1:21-cv-0024 (W.D. Ohio) (complaint filed April 8, 2021).

7 *Mondelez Intl. Inc. v. Zurich Am. Ins. Co.,* Case No. 2018-L-11008 (Ill. Cir. Ct., Cook Cty., complaint filed Oct. 10, 2018).

8 Lloyd's Market Bulletins Y5258 (July 4, 2019) and Y5277 (January 29, 2020) set out mandated timelines for all Lloyd's syndicates to implement these changes. In 2019, AIG stated that it was finalizing its transition to affirmative cyber coverage as of January 1, 2020.