

A solid yellow triangle pointing downwards, located to the left of the 'BLOGS' header.

## BLOGS

### Cyber Insurance

# Cyber Insurance: Something All Businesses Should Consider

This month, when many are working with inspiration towards their New Year's resolutions, we urge each business policyholder to set a goal fitting of our modern high-tech age: checking its cyber insurance.

Cyber insurance is something of a fluid catch-all term, but insureds generally seek it to provide coverage for computer-based perils, such as those arising from unauthorized computer access ("hacking"), malicious software ("malware"), email fraud ("phishing" or "spoofing"), network failure or inaccessibility ("ransomware"), and the resulting breach or disclosure of protected data. Such insurance can be either first-party (covering the insured's own losses arising from, say, a computer system malfunction, a disgruntled employee, or a cyber criminal) or third-party (covering the insured's liability to, say, its consumers for a data breach or the government for regulatory fines).

This month, when many are working with inspiration towards their New Year's resolutions, we urge each business policyholder to set a goal fitting of our modern high-tech age: checking its cyber insurance.

Cyber insurance is something of a fluid catch-all term, but insureds generally seek it to provide coverage for computer-based perils, such as those arising from unauthorized computer access ("hacking"), malicious software ("malware"), email fraud ("phishing" or "spoofing"), network failure or inaccessibility ("ransomware"), and the resulting breach or disclosure of protected data. Such insurance can be either first-party (covering the insured's own losses arising from, say, a computer system malfunction, a disgruntled employee, or a cyber criminal) or third-party (covering the insured's liability to, say, its consumers for a data breach or the government for regulatory fines).

Standalone cyber insurance policies are still in their infancy, with varying policy language and pricing, setting them in rather stark contrast to the standardized forms and pricing models characteristic of some other types of insurance. Perhaps because this market is still maturing, reports indicate that only half of U.S. businesses have standalone cyber insurance policies,<sup>[1]</sup> with the percentage almost certainly lower among small- and medium-sized businesses that may be least able to survive the large expenditures associated with a cyber event.

Last year, a consortium of major risk and tech companies – Aon, Apple, Cisco, and Allianz – teamed to offer discounted cyber insurance, seeking to provide a holistic approach to cyber risk management that benefits from each partner's expertise.<sup>[2]</sup> Under this bundled arrangement, a prospective insured undergoes a cybersecurity assessment by Aon, uses secured tech products and services from Apple and Cisco, and obtains a cyber insurance policy issued by Allianz. The goal is to encourage more business to sign-up for cyber coverage, including by providing incentives such as discounts for security enhancements and access to tech consulting and incident response services.

As of this writing, it appears this first-in-industry offering has not been tested in the courtroom. But perhaps even more surprising is the absolute dearth of cyber-specific case law. In one of the few reported cases, a federal district court denied coverage under a cyber policy for credit card industry fees imposed due to a consumer data breach, parsing the policy's language with the type of analysis commonly applied to other more traditional insurance.<sup>[3]</sup>

This leads to an important point: Given the novelty of cyber insurance, insurers and courts will interpret them according to the familiar legal cannons, and insureds should consider whether coverage might exist under their existing traditional insurance policies. This blog has previously advised you about an insured who unsuccessfully sought coverage under a crime-protection policy for an email spoofing fraud.<sup>[4]</sup> But thankfully, other insureds have been successful. For instance, both the Second and Sixth Circuits have found coverage for a spoofing fraud under a crime or business policy's computer fraud provision.<sup>[5]</sup>



Considering all of this, we encourage all businesses to check again their cyber security risks and coverage needs, under both cyber-specific and more generalized insurance policies. Lathrop Gage's insurance recovery team is experienced in these matters and stands ready to assist policyholders at each step of the process, from conducting proactive policy analysis to litigating high-value coverage disputes at trial and on appeal.

[1] "Why 27% of U.S. Firms Have No Plans to Buy Cyber Insurance," Insurance Journal, <https://www.insurancejournal.com/news/national/2017/05/31/452647.htm> (last accessed January 2, 2019).

[2] "Cisco, Apple, Aon, Allianz introduce a first in cyber risk management," Apple press release, <https://www.apple.com/newsroom/2018/02/cisco-apple-aon-allianz-introduce-a-first-in-cyber-risk-management/> (last accessed January 2, 2019).

[3] *P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.*, No. CV-15-01322-PHX-SMM, 2016 WL 3055111 (D. Ariz. May 31, 2016), <https://docs.justia.com/cases/federal/district-courts/arizona/azdce/2:2015cv01322/934023/45> (last accessed January 2, 2019).

[4] "Social Engineering Cyber Coverage: Protecting Your Company from the Human Factor," <https://www.roadtoinsurancerecovery.com/2018/08/social-engineering-cyber-coverage-protecting-company-human-factor/>.

[5] *Medidata Sols. Inc. v. Fed. Ins. Co.*, 729 F. App'x 117 (2d Cir. 2018), <https://www.insurancejournal.com/app/uploads/2018/07/Medidata-v-Federal-Insurance.pdf> (last accessed January 2, 2019); *Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 895 F.3d 455 (6th Cir. 2018), <https://law.justia.com/cases/federal/appellate-courts/ca6/17-2014/17-2014-2018-07-13.html> (last accessed January 2, 2019).