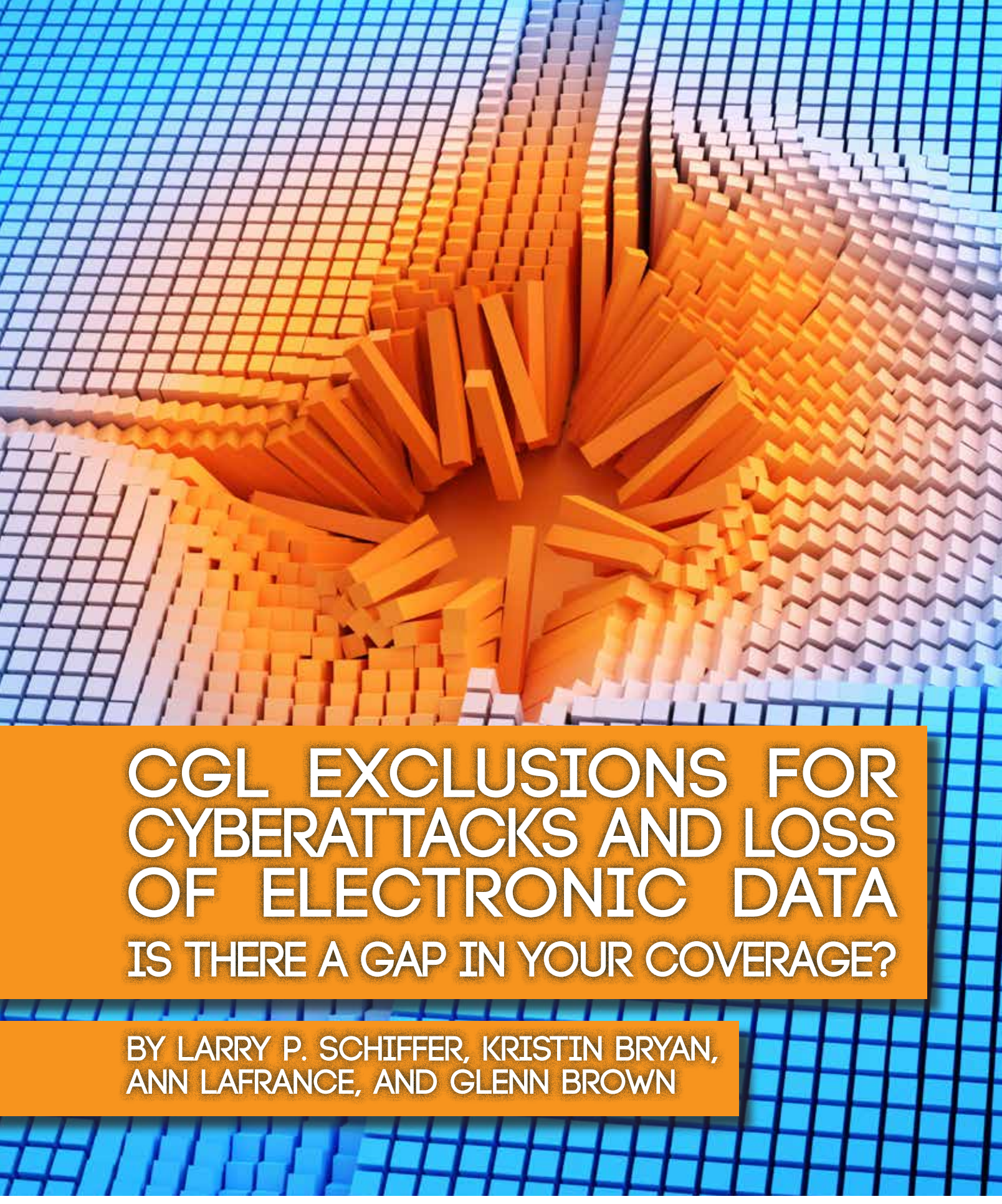


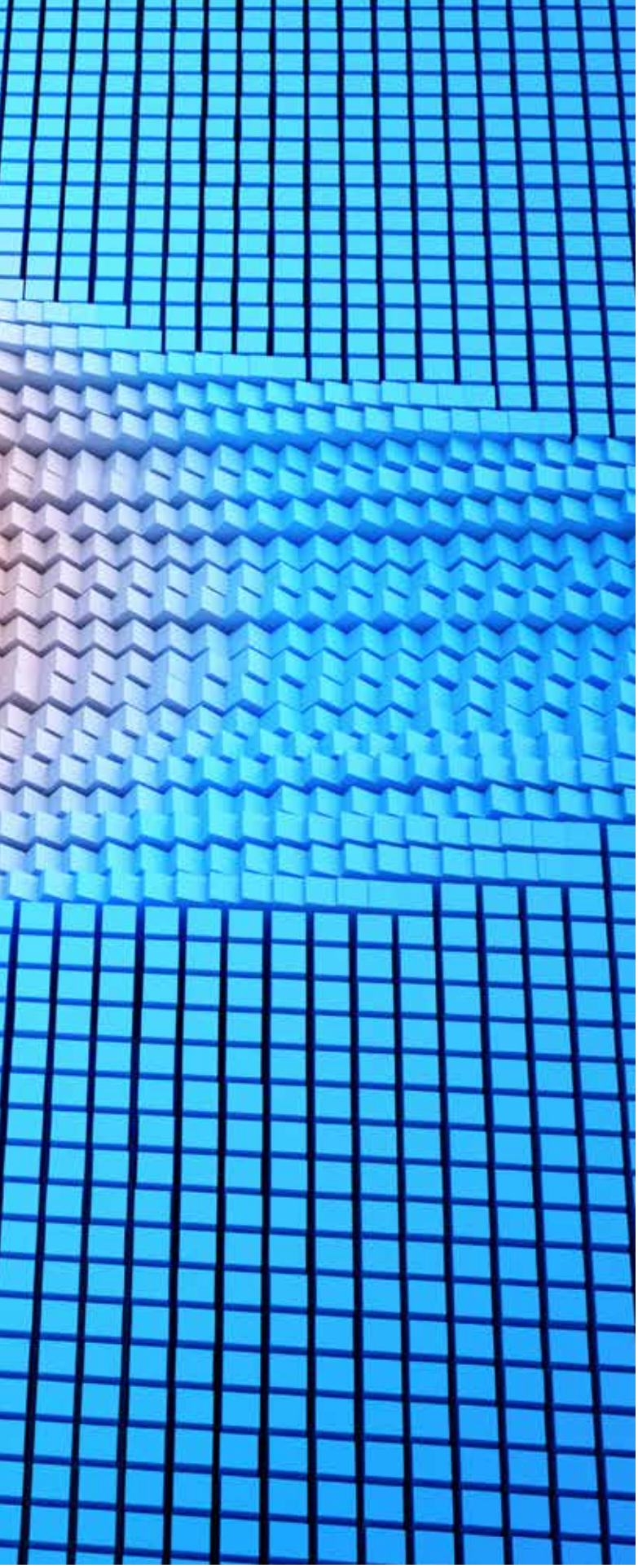
CGL EXCLUSIONS FOR CYBERATTACKS AND LOSS OF ELECTRONIC DATA

IS THERE A GAP IN YOUR COVERAGE?

BY LARRY P. SCHIFFER, KRISTIN BRYAN, ANN LAFRANCE, AND GLENN BROWN

FLORIANA / ISTOCK VIA GETTY IMAGES PLUS

PUBLISHED IN THE BRIEF, VOLUME 49, NUMBER 4, SUMMER 2020. © 2020 BY THE AMERICAN BAR ASSOCIATION. REPRODUCED WITH PERMISSION. ALL RIGHTS RESERVED. THIS INFORMATION OR ANY PORTION THEREOF MAY NOT BE COPIED OR DISSEMINATED IN ANY FORM OR BY ANY MEANS OR STORED IN AN ELECTRONIC DATABASE OR RETRIEVAL SYSTEM WITHOUT THE EXPRESS WRITTEN CONSENT OF THE AMERICAN BAR ASSOCIATION.



As the COVID-19 outbreak continues and cybercriminals seek to exploit a remote workforce, cybersecurity issues remain fundamentally important. Businesses are concerned about the cyber risks facing their organizations, due in no small part to the staggering losses that can result from a major cybersecurity incident, which can encompass not only harm from the loss of data but also reputational damage as a result of customer impacts and subsequent media attention.

Of course, technical cybersecurity safeguards and organizational preparedness for a cyber incident remain critical for an effective cybersecurity program. Adequate insurance for cyberattacks and loss of data is just as essential, however, although often overlooked. Regardless of size, every organization should assess whether it has adequate cyber liability insurance. This article explores the use of standard industry forms to cover cyber liabilities, the exclusions used in standard industry forms for data breach liability, and gaps in coverage between those standard business insurance forms and cyber liability or network security insurance policies.

Standard CGL Policies Do Not Necessarily Cover Risks Arising from Cyberattacks

The Insurance Services Office, Inc. (ISO), a Verisk company, develops form policy and endorsement language for its insurance industry subscribers. It also provides statistical, data reporting, and other services to insurers in the property and casualty industry. ISO stays current with all state insurance regulations and forms changes, and produces policy forms that purport to comply with a given state's insurance regulations as long as the current form edition is being used.

By using ISO forms, an insurance company does not have to request new state regulatory approval for its forms each time there is an update to an insurance regulation. Because carriers must obtain regulatory approval for new custom forms in most states, their use can sometimes mean considerable effort and delay, and so the convenience of using ISO forms is very appealing. Nevertheless, many insurance carriers want policies that include custom terms, so they either create custom forms incorporating segments of the ISO forms or create entirely new forms for certain coverages.

Among the policy forms developed by ISO is the familiar commercial general liability (CGL) policy. This policy provides coverage to a commercial entity for damages to and caused by the entity's business operations. Recent cases discussed below underscore the value of purchasing cyber or network security insurance to cover gaps in an organization's CGL policy. For instance, while CGL policies provide comprehensive business insurance, they do not cover all risks: CGL policies typically exclude damages arising out of losses of electronic data, which is not considered "tangible" property. As a result, many companies protect themselves from cyber-related losses with specific cyber or network security insurance policies. Various inconsistencies resulting from court decisions have also emerged, as discussed in greater detail below.

PUBLISHED IN THE BRIEF, VOLUME 49, NUMBER 4, SUMMER 2020. © 2020 BY THE AMERICAN BAR ASSOCIATION. REPRODUCED WITH PERMISSION. ALL RIGHTS RESERVED. THIS INFORMATION OR ANY PORTION THEREOF MAY NOT BE COPIED OR DISSEMINATED IN ANY FORM OR BY ANY MEANS OR STORED IN AN ELECTRONIC DATABASE OR RETRIEVAL SYSTEM WITHOUT THE EXPRESS WRITTEN CONSENT OF THE AMERICAN BAR ASSOCIATION.

TIP: To mitigate future risk, policyholders should review their CGL policies and any stand-alone cyber policies with experienced counsel to determine whether there is a gap in their coverage.

In 2013, ISO issued new endorsements to the CGL policy, which included new language regarding data-related liabilities. Nevertheless, uncertainty over coverage in this area remains. There is a disconnect between the 2013 ISO endorsements and applicable statutory law, as well as the body of case law on this issue that continues to develop.

Cyber insurance alone, however, is not a magic bullet. To mitigate future risk, policyholders should review their CGL policies and any stand-alone cyber policies with experienced counsel to determine whether there is a gap in their coverage. When a gap in coverage is identified, policyholders should immediately explore additional coverage options. With the risks posed by cyber threats and data breaches expected to continue to increase, attention to potential coverage issues arising out of these incidents should be a feature of any data protection and cybersecurity risk management program.

Early ISO Policy Forms Did Not Directly Address Data and Cyber Issues

When ISO initially developed its CGL form, hacking, data breaches, and cybersecurity risk were either nonexistent or inconsequential for most businesses. Accordingly, damage resulting from the unauthorized access, use, or disclosure of personal or confidential information was not clearly covered under older CGL policies. The many coverage disputes between insurers and policyholders over hacking and cybersecurity issues, including those that predated the release of the 2013 ISO endorsements, reflected this trend.

Larry P. Schiffer *practices commercial, insurance, and reinsurance litigation; arbitration; and mediation. He also provides consulting and expert witness services for the insurance and reinsurance industry and serves as a mediator and arbitrator. He may be reached at lpschiffer@yahoo.com.* **Kristin Bryan** *is a senior associate in the Cleveland office of Squire Patton Boggs, experienced in the efficient resolution of complex commercial and data privacy disputes and providing practical, business-oriented data privacy advice to clients. She may be reached at kristin.bryan@squirepb.com.* **Ann LaFrance** *is a partner in the New York office of Squire Patton Boggs, where she cochairs the firm's global data privacy and cybersecurity practice and is a senior member of the international communications practice. She may be reached at ann.lafrance@squirepb.com.* **Glenn Brown** *is of counsel in the Atlanta office of Squire Patton Boggs, where he provides business-oriented advice to clients in numerous industries on data privacy and regulatory compliance matters. He may be reached at glenn.brown@squirepb.com.*

As just one example, over 40 class actions were filed in 2000 against an internet services provider with proprietary software that enabled consumers to access the internet and the provider's online services. The plaintiffs, who had purchased the provider's version 5.0 access software, alleged that version 5.0 had substantial bugs and incompatibility with numerous applications and operating systems. The plaintiffs alleged that the software caused serious injury to their computer systems and preexisting software, and that version 5.0 altered the plaintiffs' existing software, disrupted their network connections, caused the loss of stored data, and caused their operating systems to crash.[1]

The provider tendered the defense of those suits to its insurance carrier, which had issued a CGL policy to the provider. The policy covered "property damage," defined as "physical damage to tangible property of others, including all resulting loss of use of that property; or loss of use of tangible property of others that isn't physically damaged."[2] The insurer denied the provider's claim because the underlying complaints did not allege damage to tangible property. In the ensuing coverage litigation, both the Eastern District of Virginia and the Fourth Circuit Court of Appeals agreed with the insurer's interpretation. The Fourth Circuit held that although the provider's CGL policy "cover[ed] any damage that may have been caused to circuits, switches, drives, and any other physical components of the computer," it did not cover "the loss of instructions to configure the switches or the loss of data stored magnetically."[3] Rather, "[t]hese instructions, data, and information are abstract and intangible, and damage to them is not physical damage to tangible property."[4]

Some courts followed the Fourth Circuit's lead in holding that damage to electronic data was not covered property damage under CGL policies. For instance, in *Recall Total Information Management, Inc. v. Federal Insurance Co.*, a Connecticut state court held that a records storage vendor that lost tapes containing the electronic data of a company in a theft did not have coverage for loss under its CGL policy.[5] The court explained that loss of electronic data did not constitute damage to "tangible property" as defined in the policy. Accordingly, there was no coverage for the claim as property damage. Similarly, in *Ward General Insurance Services, Inc. v. Employers Fire Insurance Co.*, a California appeals court held that under a commercial insurance policy, the loss of a computer database with its consequent economic loss was not a "direct physical loss of or damage to" covered property under the terms of the subject insurance policy.[6] Relying on other California precedent, the court reasoned that because the loss of the computer database was not accompanied by loss of or damage to tangible property, it was not covered.

This approach was far from uniform, however, with other courts broadly construing the terms of similar CGL policies to require coverage for damage to electronic data. For instance, in *American Guarantee & Liability Insurance Co. v. Ingram Micro Inc.*, the Arizona federal district court held that computers suffered "physical damage," as required by the CGL policy, where

PUBLISHED IN THE BRIEF, VOLUME 49, NUMBER 4, SUMMER 2020. © 2020 BY THE AMERICAN BAR ASSOCIATION. REPRODUCED WITH PERMISSION. ALL RIGHTS RESERVED. THIS INFORMATION OR ANY PORTION THEREOF MAY NOT BE COPIED OR DISSEMINATED IN ANY FORM OR BY ANY MEANS OR STORED IN AN ELECTRONIC DATABASE OR RETRIEVAL SYSTEM WITHOUT THE EXPRESS WRITTEN CONSENT OF THE AMERICAN BAR ASSOCIATION.

information stored in the computers' memory was destroyed.[7] The court reasoned (in reliance on authority from Connecticut and Minnesota) that "physical damage" was "not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality."[8] Because a "computer system and world-wide computer network physically lost the programming information and custom configurations necessary for them to function," these losses constituted physical damage for purposes of the CGL policy.[9]

2013 ISO Endorsements Address Data-Related Liabilities

In response to this ambiguity and coverage uncertainty, ISO issued new form endorsements in 2013 that added data breach liability exclusions to its standard CGL forms to clarify the CGL policy's coverage grants in this area.

ISO endorsement CG 21 06 05 14 adds an exclusion to CGL coverage A, which replaces exclusion 2.p. under "Bodily Injury and Property Damage Liability." The exclusion, under the caption "Access or Disclosure of Confidential or Personal Information and Data-Related Liability," states that the CGL policy does not cover damages arising out of "[t]he loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." The exclusion defines "electronic data" to include "information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software . . . which are used with electronically controlled equipment." The exclusion does contain limited coverage for bodily injury caused by data-related perils by including an exception for "damages because of 'bodily injury.'" ISO endorsement CG 21 07 05 14 contains identical language but does not include the limited bodily injury exception. Thus, policyholders have a choice between ISO endorsement CG 21 06 05 14 and ISO endorsement CG 21 07 05 14 regarding the purchase of the limited bodily injury exception.

Finally, ISO endorsement CG 21 08 05 14 adds an exclusion to CGL coverage B for "Personal and Advertising Injury Liability." Specifically, coverage is removed for liability arising from any access to or disclosure of "nonpublic information," including damages "claimed for notification costs, credit monitoring expenses, forensic expenses, . . . or any other loss, cost or expense . . . arising out of any access to or disclosure of any person's or organization's confidential or personal information."

Rise of Privacy Laws after Creation of 2013 ISO Endorsements

The 2013 ISO endorsements to the CGL policy preceded important developments in data privacy and protection, including enactment of the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act of 2018. Unsurprisingly, there appears to be a disconnect between the 2013 ISO endorsements and applicable data privacy statutes, including not only laws enacted after the 2013 ISO endorsements but also earlier state data breach statutes. As just one example, ISO endorsement CG 21 06 05 14 excludes damages arising out of "[t]he loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." Many of the U.S. state data breach statutes, however, define a breach as including the "unauthorized acquisition" of personal information.[10] The GDPR's definition of "personal data breach" is even broader in scope.[11] This disconnect raises possible coverage questions about whether the "unauthorized acquisition" of electronic data, in the absence of any accompanying loss, is an "occurrence."[12]

When ISO initially developed its CGL form, hacking, data breaches, and cybersecurity risk were either nonexistent or inconsequential for most businesses.

Additional coverage complexities may also arise in the context of regulatory enforcement actions for data breaches, including the imposition of fines by state attorneys general for statutory violations and whether insurance policies cover these fines under the policies themselves or in line with applicable laws and public policy.

Ambiguities Remain Because of Gaps in 2013 ISO Endorsements' Language

Because ISO provides advisory services to property and casualty insurers (and therefore adherence to ISO CGL form policies is not required), it is difficult to obtain metrics on how these endorsements are being used in practice. Carriers that incorporate the 2013 ISO endorsements in their CGL policies likely will argue that they do not cover property damage claims resulting from computer hacks or other cybersecurity incidents. As a general matter, exclusions in CGL policies are interpreted narrowly.[13] While courts may limit the scope of the 2013 ISO endorsements, coverage disputes are of course resolved on a case-by-case basis, making no outcome guaranteed.

In *Camp's Grocery, Inc. v. State Farm Fire & Casualty Co.*, there was a coverage dispute regarding underlying litigation

PUBLISHED IN THE BRIEF, VOLUME 49, NUMBER 4, SUMMER 2020. © 2020 BY THE AMERICAN BAR ASSOCIATION. REPRODUCED WITH PERMISSION. ALL RIGHTS RESERVED. THIS INFORMATION OR ANY PORTION THEREOF MAY NOT BE COPIED OR DISSEMINATED IN ANY FORM OR BY ANY MEANS OR STORED IN AN ELECTRONIC DATABASE OR RETRIEVAL SYSTEM WITHOUT THE EXPRESS WRITTEN CONSENT OF THE AMERICAN BAR ASSOCIATION.

brought by three credit unions against a policyholder following a computer hack.[14] The credit unions alleged that due to the policyholder's lax security practices, they suffered losses on their cardholder accounts, "including for reissuance of cards, reimbursement of their customers for fraud losses, lost interest and transaction fees, lost customers, diminished good will, and administrative expenses associated with investigating, correcting, and preventing fraud."[15] Mirroring the exclusionary language in the 2013 ISO endorsements, the policyholder's CGL policy expressly excluded "electronic data" from the definition of "covered property" and did not provide coverage for "damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[16] Assessing both the CGL policy as well as two endorsements attached to the policy, an Alabama federal district court found that the insurer had no duty to defend or indemnify the credit unions' claims that did not involve "property damage" as defined in the policy.[17]

Most cyber insurance policies exclude claims for bodily injury and property damage, even though those claims may not be covered by the insured's CGL policy—therein lies the gap.

In *Country World Media Group, Inc. v. Erie Insurance Co.*, however, the Wisconsin Court of Appeals held that an insurer had a duty to defend its insured in litigation brought by a third-party media company for the insured's alleged breaches of contract and negligence.[18] The company alleged damages for both the loss of intangible data contained on videotapes and the loss of the tapes themselves on which television shows, master copies, and field footage were stored, caused by the insured's destruction of the materials. Under the terms of the insured's CGL policy, while property damage was covered, the policy expressly excluded "electronic data" from the definition of covered property and "[d]amages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[19] The court concluded that the loss of the physical tapes constituted property damage, as the policy defined that term, and was therefore covered, without addressing whether the content of the tapes themselves constituted "electronic data" under the policy.[20]

Recent Developments Add to This Body of Law

More recent decisions, including some issued this year, continue to refine this area of the law, but uncertainty remains.

In 2018, the Sixth Circuit Court of Appeals held that an insured's losses after a phishing attack were covered under a cyber insurance fraud policy.[21] Specifically, the Sixth Circuit held that the district court erred in granting summary judgment to the insurer, finding that an insured's business insurance policy did not cover its loss stemming from fraudulent emails that caused it to wire money to a party impersonating its Chinese vendor. The court reasoned that the insured suffered a "direct loss" as it immediately lost its money when it transferred the funds to the impersonator, which constituted "computer fraud" as these terms were defined in the policy at issue.[22]

The Sixth Circuit's decision was issued in the wake of *Medidata Solutions, Inc. v. Federal Insurance Co.*, in which the Southern District of New York became the first federal court to hold that data loss after a phishing attack was covered under a cyber insurance policy.[23] The Second Circuit Court of Appeals affirmed the district court's ruling.[24]

Again, however, this approach is far from uniform. The Fifth and Ninth Circuit Courts of Appeals have denied coverage under comparable circumstances.[25]

This year, in *National Ink & Stitch, LLC v. State Auto Property & Casualty Insurance Co.*, the Maryland federal district court ruled that lost data and the compromised operability of a computer system resulting from a cyberattack qualified as "direct physical loss" under a first-party property policy.[26] *National Ink & Stitch* concerned a 2016 ransomware attack on an online screen printing and embroidery company. This attack prevented the company from accessing practically all of its software and files on its servers. After receiving the ransom payment, the hacker refused to decrypt the servers and demanded an additional payment. Instead of making the additional payment, the company hired a security vendor to replace its IT system entirely with new servers and computers and then sought coverage for the replacement costs under its business owners' property insurance policy. The carrier denied coverage for the replacement costs, and the company filed suit.[27]

Both parties moved for summary judgment on the issue of whether the company's loss of data and the impairment of its system constituted "direct physical loss" within the coverage of the policy. In ruling for the policyholder, the court noted that the policy included "[e]lectronic data processing, recording or storage media such as films, tapes, discs, drums or cells" and "[d]ata stored on such media" within the definition of "covered property."[28] This definition was significant to the court, which applied principles of contract interpretation in addressing the parties' dispute.

PUBLISHED IN THE BRIEF, VOLUME 49, NUMBER 4, SUMMER 2020. © 2020 BY THE AMERICAN BAR ASSOCIATION. REPRODUCED WITH PERMISSION. ALL RIGHTS RESERVED. THIS INFORMATION OR ANY PORTION THEREOF MAY NOT BE COPIED OR DISSEMINATED IN ANY FORM OR BY ANY MEANS OR STORED IN AN ELECTRONIC DATABASE OR RETRIEVAL SYSTEM WITHOUT THE EXPRESS WRITTEN CONSENT OF THE AMERICAN BAR ASSOCIATION.

The court held that the computer equipment impaired by the ransomware attack qualified as covered property because it contained hard drives and could not be used for electronic data processing, recording, or storage after the attack. In rejecting the carrier's argument to the contrary, the court ruled that complete inoperability was not required because the policy protected against "damage to" covered property in addition to "physical loss."[29]

Cyber Insurance Is Not a Magic Bullet to Cover Gaps in a CGL Policy

These cases underscore the value of purchasing cyber or network security insurance to cover gaps in an organization's CGL policy and the paramount importance of precision in policy language. Cyber insurance alone, however, is not a magic bullet, and organizations that have cyber insurance may not be as protected as they believe themselves to be. Most cyber insurance policies exclude claims for bodily injury and property damage—even though those claims may not be covered by the insured's CGL policy, as seen from the above examples. Therein lies the gap.

Underscoring the disconnect, in July 2019, one of the world's largest commercial property insurers conducted a survey of chief financial officers (CFOs) at companies with over $1 billion in revenue.[30] Of the CFOs surveyed, 71 percent understood that their insurer would cover "most" or "all" of the damages their company would incur in a cyberattack. Many of the effects the CFOs expected to experience in a material cybersecurity event (such as issues arising from increased investor scrutiny), however, are not typically covered by cyber insurance policies.[31]

To mitigate future risk, policyholders should at a minimum review their CGL policies and any stand-alone cyber policies with experienced counsel to determine whether there is a gap in their coverage. If a gap in coverage is identified, policyholders should immediately explore additional coverage options. With the risks posed by cyber threats and data breaches expected to grow as more and more companies adopt work-from-home policies and reliance on online and cloud-based services increases, attention to potential coverage issues arising out of these incidents is critical. ◄

Notes

1. Am. Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89, 93 (4th Cir. 2003).
2. *Id.* at 94.
3. *Id.* at 96.
4. *Id.*
5. No. 095031734, 2012 Conn. Super. LEXIS 227, at *17 (Jan. 17, 2012).
6. 7 Cal. Rptr. 3d 844, 851 (Ct. App. 2003).
7. No. 99-185, 2000 U.S. Dist. LEXIS 7299, at *2 (D. Ariz. Apr. 18, 2000).
8. *Id.* at *5.
9. *Id.* at *8; *see also* Ashland Hosp. Corp. v. Affiliated FM Ins. Co., No. 11-16, 2013 U.S. Dist. LEXIS 114730, at *1 (E.D. Ky. Aug. 14, 2013) (holding that the corruption of computer data and loss in "long term reliability" of a data storage network constituted "direct physical loss or damage" under the policy); Se. Mental Health Ctr., Inc. v. Pac. Ins. Co., Ltd., 439 F. Supp. 2d 831, 833–34 (W.D. Tenn. 2006) (holding that the corruption of the pharmacy computer constituted "direct physical loss of or damage to property" under a business interruption policy).
10. *See, e.g.*, Mo. Rev. Stat. § 407.1500.
11. *See* Commission Regulation 2016/679, art. 4, 2016 O.J. (L 119) 1.
12. *See, e.g.*, Cal. Civ. Code § 1798.82; Minn. Stat. § 325E.61; S.C. Code Ann. § 39-1-90.
13. *See, e.g.*, Taos Ski Valley, Inc. v. Nova Cas. Co., 705 F. App'x 749, 753 (10th Cir. 2017) (applying insurance policy exclusionary language narrowly in accordance with applicable state law).
14. No. 4:16-cv-0204, 2016 U.S. Dist. LEXIS 147361, at *2 (N.D. Ala. Oct. 25, 2016).
15. *Id.*
16. *Id.* at *6.
17. *Id.* at *24.
18. No. 2016-1343, 2017 Wis. App. LEXIS 312, at *1–2 (May 2, 2017).
19. *Id.* at *9.
20. *Id.* at *10–11.
21. Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 457 (6th Cir. 2018).
22. *Id.* at 462–63.
23. 268 F. Supp. 3d 471 (S.D.N.Y. 2017).
24. *See* Medidata Sols. Inc. v. Fed. Ins. Co., 729 F. App'x 117 (2d Cir. 2018).
25. *See, e.g.*, Taylor & Lieberman v. Fed. Ins. Co., 681 F. App'x 627 (9th Cir. 2017) (denying coverage of a computer fraud provision when an accounting firm fell victim to an email spoofing scam after a criminal invaded the email account of the accounting firm's client and sent emails requesting wire transfers); Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252 (5th Cir. 2016) (holding that the insured's loss was not a covered occurrence under the computer fraud provision of its crime protection insurance policy because while an email was part of the criminal scheme, it was merely incidental to the occurrence of the authorized transfer of money).
26. No. SAG-18-2138, 2020 U.S. Dist. LEXIS 11411 (D. Md. Jan. 23, 2020).
27. *Id.* at *1–4.
28. *Id.* at *3–4.
29. *Id.* at *16.
30. *See* Press Release, FM Glob., Cyber Insurance May Create False Sense of Security among Senior Financial Executives at World's Top Companies, Suggests FM Global Survey (July 30, 2019), https://newsroom.fmglobal.com/releases/cyber-insurance-may-create-false-sense-of-security-among-senior-financial-executives-at-worlds-top-companies-suggests-fm-global-survey.
31. *Id.*

PUBLISHED IN THE BRIEF, VOLUME 49, NUMBER 4, SUMMER 2020. © 2020 BY THE AMERICAN BAR ASSOCIATION. REPRODUCED WITH PERMISSION. ALL RIGHTS RESERVED. THIS INFORMATION OR ANY PORTION THEREOF MAY NOT BE COPIED OR DISSEMINATED IN ANY FORM OR BY ANY MEANS OR STORED IN AN ELECTRONIC DATABASE OR RETRIEVAL SYSTEM WITHOUT THE EXPRESS WRITTEN CONSENT OF THE AMERICAN BAR ASSOCIATION.