2022 Insurance & Professional Liability Seminar

June 22-24, 2022

DEFENDING AFTER DATA GOES DOWN:

The Perils and Pitfalls of Data Breaches

Todd Lubben
Moderator
BROWN & JAMES, P.C.
St. Louis, Missouri
tlubben@bjpc.com

Kate Whitlock
HAWKINS PARNELL &
YOUNG, LLP
Atlanta, Georgia
kwhitlock@hpylaw.com

There are four main types of data breaches. Make no mistake: one of them will personally affect each and every professional.

- Hacker attack: An attempt to disable computers, steal data, or use a breached computer system to launch additional attacks. Cybercriminals use different methods to launch such a cyberattack, including malware, phishing, ransomware, man-in-the-middle (perpetrator positions himself in a conversation between a user and an application, either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway), and password theft.
- Physical theft and/or loss of device: Theft of hard copies of medical or financial records, laptops, cell phones, tablets, and other devices.
- Data theft/leak**:** Exposure of sensitive data to the public**,** sometimes internally by a disgruntled employee or former employee with retained passwords or stolen confidential company data.
- Human error: Inadvertent disclosure of protected information by, for example, mis-sent e-mail, falling for phishing attacks (thus providing passwords or other sensitive company information to criminals), and wiring funds in accord with fraudulent instructions.

While the company CGL policy is unlikely to provide coverage for data breaches, courts have ruled that, in certain limited circumstance, a CGL policy will provide data breach coverage. See *Landry's Inc. v. Insurance Company of the State of Pennsylvania*, 4 F.4th 366 (5th Cir. 2021). Most courts recognize, though, that a data breach does not involve bodily injury or property damage caused by an accident so it will not fall within the policy definition of an occurrence. (Coverage A). Likewise, a data breach does not fall within any of the items listed under the personal and advertising injury coverage (Coverage B). Furthermore, for avoidance of doubt, many CGL policies now contain a specific exclusion for cyber-related claims.

Every company needs data breach coverage, either stand alone or as part of a cyber policy. The data breach policy should cover:

First Party coverage:

- Charges for the cost of notification and identity and credit monitoring
- Public relations consulting as assistance
- Data loss, data recovery and data recreation
- Cyber extortion
- Funds transfer fraud
- Loss of revenue from business interruption
- Computer forensic investigation and analysis

Third Party coverage:

Businesses can be sued for damages for a data breach for failing to properly protect data that includes proprietary information of a third party. *See, e.g., Silverpop Sys. v. Leading Mkt. Techs., Inc.*, 2014 U.S. Dist. LEXIS 185346 (N.D. Ga. 2014). If you share data with a third party and that party has a data breach, your company can be sued as a result.

The third-party coverage in the data breach policy should cover:

- The cost of responding to regulatory inquiries

- Fines and penalties resulting from a government inquiry
- Defense costs of a data breach lawsuit
- Any damages awarded as the result of a data reach lawsuit
- The cost of settling a data breach lawsuit

The data breach policy should include access to data breach risk management and mitigation tools and resources.

The resources provided by the policy should include a call-in number for data breach advice pre and post breach. Information should be provided for public relations and advertising support, credit monitoring and identity theft restoration, breach notification, IT security and access to forensic experts.

The risk to professionals of having a cyberbreach was increased by the move from all in-office to hybrid or remote work. Employees using home wireless networks and public wifis are not protected by company firewalls, updates, and security programs. Employees also use personal devices for work which increases risk, even if it is just to transfer files. This means that employees may retain confidential information upon leaving the company even if they turn in all their company-provided devices. Also, employees may be less vigilant with security measures when they are working from home or another venue because the environment is more relaxed. *Most Common Remote Work Security Risks* (July 2021), https://heimdalsecurity.com/blog/cybersecurity-issues-with-remote-work/.

There are also physical security issues that arise from remote work settings. If there are other people present in a home office environment, it may be difficult or impossible to have a private telephone conversation. Similarly, someone in a café may inadvertently share information to others simply by having a computer screen opens as someone else walks by. *Cyber Security Risks: Best Practices for Working from Home and Remotely*, https://usa.kaspersky.com/resource-center/threats/remote-working-how-to-stay-safe.

Companies, firms, and individuals need to consider these new risks, create policies to address them and take personal responsibility for them. *The cyber security risks of working from home* (Aug. 2021), https://www.itgovernance.co.uk/blog/the-cyber-security-risks-of-working-from-home. A remote work policy should consider guidance on storing devices securely, creating and maintaining strong passwords, visiting websites that aren't work-related, and an explanation of the technical solutions to protect sensitive data. The need to be hyperaware of these problems is evident from the litigation over cyber issues.

Last year, the litigation in this area continued to focus on the issues of standing and discovery. On the standing, the Supreme Court in *Ramirez v. Transunion*, 141 S. Ct. 2190 (2021), in which the Supreme Court said that, where the vast majority of a putative class suffered no actual injury, let alone the type of injury suffered by a class representative, no standing to sue existed. The Supreme Court further declared that "the mere risk of future harm, without more, cannot qualify as a concrete harm in a suit for damages." *Ramirez* at 2210-2211.

That did not close the question or stop the litigation. After that, an Arizona District Court found that an alleged risk of future harm that were "certainly impending" was enough to confer standing. *Griffey v. Magellan Health Inc.*, 2021 U.S. Dist. LEXIS 184591 (D. Az. 2021); *Burns v. Mammoth Media, Inc.,* 2021 U.S. Dist. LEXIS 149190 (C.D. Ca. 2021) (stolen data was "essentially useless" so Plaintiff was not damaged and had no standing). *But see*, *Legg v. Leaders Life Ins. Co.*, 2021 U.S. Dist. LEXIS 232833 (W.D. Okla. 2021) (allegations of *general* risks of harm did not suffice to allege standing). It thus appears that the rule is a risk of future harm plus. *Stewart v. Kendall, Secretary of the Air Force, et. al.*, 2022 U.S. Dist. LEXIS 1203 (D.C. 2022) (mitigation costs incurred to prevent future injury constitutes damages for purposes of standing); *Mackey v. Belden, Inc.*, 2021 U.S. Dist. LEXIS 145000 (E.D. Mo. 2021) (theft of Social Security number coupled with the filing of a false tax return after the theft was sufficient to confer standing); *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332 (11th Cir. 2021) (to show standing,

plaintiff must have concrete and particularized injury that was actual or imminent); *Abernathy v. Brandywine Urology Consultants, P.A.*, 2021 Del. Super. LEXIS 46 (2021) (mere notice of a data breach even coupled with speculative future harm is insufficient to confer standing). But, *Cf., Burns v. Mammoth Media, Inc*., 2021 U.S. Dist. LEXIS 149190 (C.D. Cal. 2021) (plaintiff must show actual connection between damages and the breach); *Collins v. Athens Orthopedic Clinic*, 356 Ga. App. 776 (2020) (allegations that personal data was stolen on a mass scale by a criminal, who in turn offered it for sale to other criminals, who could assume plaintiffs' identities and fraudulently obtain credit cards, issue fraudulent checks, file tax refund returns, liquidate bank accounts, and open new accounts in their names were sufficient to state a claim).

Once the plaintiffs are in place, one must consider who to name as defendants. Recently there have been claims against directors and officers arising out of their responses to data breaches. Infamously, there was Joseph Sullivan of UBER who was charged with obstruction of justice and misprision of a felony for his data breach response. *United States v. Sullivan*, Case No. 3-20-71168-JCS (N. D. Ca. 2020). And earlier this year, Hiscox took to trial its claims against a law firm arising out of the law firm's response to litigation. *Hiscox Ins. Co. Inc. et al v. Warden Grier LLP*, No. 4:20-cv-00237 (W.D. Mo. 2020). While the law firm prevailed, no one need to explain the cost to the law firm of having been named.

Finally, after the parties are named and litigation is underway, discovery issues will arise. Recently, the issue of interest is discoverability of cyber expert reports. In *In re Capital One Consumer Data Security Breach Litigation* (Capital One), 2020 U.S. Dist. LEXIS 91736 (E.D. Va. 2020), Capital One claimed that a report on a data breach prepared by Capital One's pre-established security consultant was privileged. The Court disagreed. It analyzed Capital One's business relationship with the consultant as well as earlier reports prepared for cybersecurity purposes. The Court then decided that the at-issue report would have been prepared in the same way even if there had not been litigation. Therefore, the report did not meet the "because of" litigation standard for work product protection. There was no discussion about whether the report would be protected under the attorney-client privilege as work essentially prepared by the litigation counsel's expert or paralegal in accord with the *United States v. Kovel*, 296 F.2d 918 (1961) standard. Just a few months later, the D.C. circuit agreed. *Wengui v. Clark Hill, PLC*, 338 F.R.D. 7 (D. D. C. 2021). This was followed shortly by *In re Rutter's Data Security Breach Litigation*, 2021 U.S. Dist. LEXIS 136220 (M.D. Pa. 2021) in which the Court held that a report about whether the breach resulted in the compromise of sensitive data from a cyber investigation company hired by outside counsel was not privileged.

To reduce the chance that a court finds no privilege, consider carefully who should have access to information. Fewer people being involved will increase the legal protections. Look at the roles, authorities, and capacities of participants and tighten the group to only those who need to know information for legal reasons. Inclusion of too many people may undermine legal protections on work performed on a specific legal case.

Also, make it clear that the third-party expert was "translating" complex subject matter and not merely supplying facts. Have the attorney direct the actions of third party and funnel all communications, including billing, through the lawyer. Have a robust and clear engagement letter for the incident at-issue with the cyber expert that sets out the scope and terms of engagement. Segregate the expert's file from other cyber work product, in a place specified for the litigation. Use privilege labels to identify the sensitive work of the expert as work product and privileged and avoid labels for ministerial communications.

To avoid security breaches in the first instance, consider the people.

DO:

1. Implement continuous training

2. Identify protected communications and information
3. Prioritize privacy and cybersecurity
4. Keep records

DO NOT:

1. Overshare
2. Ignore opportunities to strengthen relationships and contractual language regarding cybersecurity
3. Produce communication or information without input from legal and insurance advisors
4. Next, consider the technology.

DO:

1. Maintain security
2. Use encryption
3. Secure mobile devices with remote wiping for lost or stolen equipment
4. Mark privileged, confidential, and work-product documents
5. Save files to secure server not mobile devices
6. Create client portals for exchanging sensitive and privileged information
7. Mark messages and attachments as Attorney-Client Privilege
8. Use encryption for sensitive messages
9. Maintain security for systems and all devices

DO NOT:

1. Save or download to mobile devices or local drives on laptops
2. Share passwords with others
3. Use weak or long-standing passwords
4. Ignore your training

In addition, professionals should keep in mind other potential regulators of data.

Health Insurance Portability and Accountability Act (HIPAA), established by the Department of Health and Human Services. The Office of Civil Rights audits healthcare providers. Violations are subject to penalties and mandatory reporting needs to occur within 60 days. Implementation of Business Associate Agreements and proper execution of disclosures for authorized release of information are at issue.

Credit card issuers covering online transactions are monitored by the Payment Card Industry Data Security Standard (PCI DSS). Transactions are subject to point-in-time audits for security. Security measures recommended for all mobile devices. Data encryption before receipt by device, such as Point-to-Point Encryption, suggested.

The Federal Communications Commission (FCC) regulates communications. The Food and Drug Administration (FDA) oversees patient safety for mobile medical devices.

Sarbanes-Oxley (SOX) compliance for publicly held companies, financial/insurance touches. Variety of audits for security assessments for privacy protections.