This article was originally published in Enforce *(Volume 13, Issue 1)*

Enforce
The Insurance Policy Enforcement Journal

Cyber Claims Insurance Protection is Tricky Business

By David E. Wood and Joshua Gold

While the risks posed by data breaches are by now widely recognized, effective management of the risk is lagging. Statistics from PwC's 2015 Global State of Information Security Survey indicate that concern about data breaches is up, yet half of all businesses have no plans to dedicate more resources to avert these perils. The purchase of dedicated cyber insurance products appears to be on the rise, but according to a new study from the Ponemon Institute many in the insurance brokerage community indicate that the marketplace is not yet as robust as one would expect given the staggering scope of recent data breaches and the ensuing headlines.[1]

Figuring out what kind of insurance is needed to respond effectively to cyber claims is challenging. For example, a recent decision from a federal court in Utah ruled that a Travelers CyberFirst liability insurance policy (marketed by Travelers as "a flexible approach to meet many of the specialty insurance needs of today's innovative technology companies")[2] did not cover a claim involving a corporate policyholder's alleged failure to return stored data for a client. The trial court ruled that the policyholder was not entitled to a defense under the cyber liability insurance policy against a client lawsuit specifically alleging misconduct in the handling of data entrusted to the policyholder — a risk the policyholder likely thought it was buying insurance for. *Travelers Property Casualty Company of America et al. v. Federal Recovery Services et al.*[3] The court not only found that the loss was outside the coverage of the policy, it held that

---

David E. Wood is editor of *Enforce* magazine and a co-managing shareholder in the Ventura, California, office of Anderson Kill. With 30 years of experience in the insurance industry, Mr. Wood devotes his practice to the representation of corporate and public entities in insurance recovery matters involving primary and excess liability and errors and omissions coverage, professional liability insurance, cyber coverage, crime coverage, environmental coverage, and rights of additional insureds.
(805) 288-1300 | dwood@andersonkill.com

Joshua Gold is a shareholder in the New York office of Anderson Kill and chair of the firm's Cyber Insurance Recovery Practice Group. Mr. Gold's practice involves matters ranging from international arbitration, data security, directors and officers insurance, business income/property insurance, commercial crime insurance, and insurance captives. He has been lead trial counsel in multiparty bench and jury trials, and has negotiated and crafted scores of settlement agreements including coverage-in-place agreements.
(212) 278-1886 | jgold@andersonkill.com

there was no possibility whatsoever of coverage being triggered by the client's claim. In short, given this court's ruling, there was a complete disconnect between the allegations of the complaint and the language of the policy, indicating that the policyholder's attempt to insure its cyber liability exposure by purchasing Travelers CyberFirst had been an utter failure.

Recent history teaches us further that the losses occasioned by cyber security breaches are not always predictable. The Sony Pictures breach is a prime example, as it imperiled or implicated in one fell swoop proprietary and intellectual property, employee personal information, sensitive management communications, reputation/goodwill, extortion, threats of bodily injury and business income.[4] Now that hackers are extending the playing field of targeted data beyond the familiar categories of customer credit card numbers, addresses and health-related data, risk managers need to reprioritize certain protections[5] (including insurance protection) that used to be lower down on the shopping list. For example, reputational and business income coverage becomes more important in hacks like that which targeted Sony Pictures.

Another example of the expanding risk involved a recent cyber attack on a European airline's ground operations system that halted certain flight operations.[6] Doubtless, this hack caused business interruption losses for the airline.

Further widening the scope of cyber claims, D&O insurance came into the picture last year after data breaches spurred derivative lawsuits against company directors and officers.[7] While cyber insurance products are finally registering on the radar of senior corporate executives, D&O insurance policies remain nearest and dearest to directors' and officers' hearts. It is therefore essential that D&O insurance responds to suits targeting company managers and directors that have their genesis in data breaches.[8]

Purchasing adequate insurance coverage for technology-related insurance claims is challenging, as products lack uniformity and the claims history is thin. Following the 10 tips below will improve the chances of recovery from stand-alone cyber and D&O insurance policies.

1. Pursue Clarity

Buy an insurance policy that you can actually understand. Unfortunately, many cyber insurance policies are virtually incomprehensible. Since there is not a lot of uniformity of product in the marketplace right now, many policies are confusing and densely written, making it hard to determine the scope of actual protection provided. Also, comparison shop with a good insurance broker at your side to help you find the best forms.[9]

Once you have a good, comprehensible form to work with, the insurance company will often endorse it to provide protection that is better tailored to your needs if you know what to ask for. Choose a broker with a lot of experience with cyber insurance products to assist in this process.

2. Cover the Evolving Risk

Continuously monitor trends in computer hacks and data breaches. Remember that data breaches can still occur the old fashioned way through theft of sensitive hard-copy documents, as well as in cutting-edge ways not currently imagined.[10] Your insurance policy needs to match the underlying exposure.

3. Cover Time-Element Losses

Business income coverage and reputational damage coverage take on added importance in the wake of recent hacking events.[11] While a slew of insurance companies have offered

cyber coverage for business income losses and reputational damage for several years, that coverage was not nearly as coveted as class action privacy litigation coverage, breach notification costs or regulatory proceedings coverage.[12] Now, the reality that a breach can imperil the very core of the policyholder's ability to continue business operations takes on much greater import for risk management objectives. As such, consider insurance coverage that pays time-element claims resulting from reputational damage and business interruptions, including ones that partially interfere with business income.[13]

4. Seek Retroactive Dates

Push for retroactive coverage whenever possible. Many insurance companies want to provide insurance protection only from the date that the first policy they sold you incepts. The problem is that some cyber threats occur well before the policyholder actually learns of them. Computer forensic specialists will tell you that computer hackers can intrude into a computer system weeks, months, and even years before the policyholder becomes aware of the threat. You can avoid disputes by negotiating with your insurance company for a retro date that pre-dates policy inception.[14]

If you purchase insurance coverage with a retroactive date that pre-dates the policy period, your cyber insurance company may ask you to provide a warranty letter.[15] If you provide one, make sure it is carefully written and ensure that you do your due diligence in reaching out to other departments and employees within the company to ensure that your representations are fair.

Policyholders can expect that any statement warranted or otherwise set forth to the insurance company will be scrutinized by the insurance company should an insurance claim ensue after the letter. As such, policyholders should not "over-promise" in the letter. State what you can after a reasonable internal inquiry. When at all possible, try to underscore to other employees and departments within the organization the importance of bringing claims or circumstances that may reasonably be viewed as likely to result in claims to the attention of the risk management and/or law department. This process can be fostered further by establishing clear written protocols within an organization of the circumstances that should be reported to risk management and legal personnel. Routine reminders of the policyholder's procedures are important too so that new hires are firmly aware of the protocols and existing employees are provided frequent reminders.

5. Avoid Breach of Contract and Warranty Exclusions

Resist efforts to include breach of contract exclusions in your coverage. These provisions should be obsolete in an era in which so many policyholders do business pursuant to a contract (whether with customers, credit card companies, financial institutions, etc.). These exclusions are used all the time by some insurance companies to challenge insurance claims. While some recent court decisions have curtailed this use, it is best not to have this fight in the first place.[16]

6. Avoid Cyber Security Reasonableness Clauses

Resist insurance company efforts to include exclusions, warranties, representations or "conditions" in insurance policies concerning the soundness or reasonableness of the policyholder's data security efforts/protocol. These clauses are a recipe for disputes on potentially every security incident.[17]

Given the pace of technological innovation, almost every security step can be second-guessed with the benefit of 20-20 hindsight. Is it safe to log onto a secure network from your hotel room using the hotel's Wi-Fi? Is it ever OK to have any unencrypted information stored on a mobile device? What about unencrypted information on the cloud? The answers depend on many factors that are difficult to pinpoint, including the devel-

opment of alternative technologies, the trends of cybercrime, the burdensomeness upon necessary business tasks compared with the need to secure data, and the exact point in time in which attitudes collectively begin to change. Such questions are bound to end in disputes if the cyber claim is big enough.

7. Preserve D&O Insurance Coverage for Cyber Claims

Keep your directors and officers insurance program (primary, excess, Side A, etc.) clean from any cyber-related exclusions or sublimits. Management and the board will be highly concerned with any argued "gap" in coverage should a cyber event ensue and D&O coverage be contested on the basis of an exclusion or limitation for suits where cyber may be the underlying cause or context of the claim. Indeed, the Securities and Exchange Commission is very concerned that public companies carefully consider cyber risks and has continued its dialogue on the matter for the last few years.[18]

8. Be Thorough When Filling Out Cyber Insurance Policy and D&O Policy Applications

Complete insurance applications carefully and gather information from other business units where necessary when answering questions. Even if an insurance company must pay a claim under the plain terms of the insurance policy, coverage may still be contested, under certain circumstances, on grounds that application questions were not correctly answered. Do not give the insurance company this opportunity.[19]

9. Remember That Cyber Breaches Happen Off-Line Too

Make sure your cyber-specific coverage protects losses involving mobile devices, home offices, data that is off-line at the time security is breached and devices that may not be owned by the policyholder. A lost laptop or flash drive containing gigabytes of information can lead to a breach and possibly an expensive one.[20] Make sure your insurance coverage is available for such a scenario — even where the device is not actively connected to a network when the data breach occurs.

10. Cover Cloud and Third Party Vendors

Make sure that your cyber-specific coverage protects against losses where others manage, transmit or host data for your company.[21] Insurance coverage is available for cloud computing and instances where data is handled, managed or outsourced to a third party. Going back to point number one above, however, not all insurance policies are created equal and there are cyber insurance forms that on their face, appear not to provide express protection for cloud-like scenarios. Most of these policies can be modified to extend such protection — *if requested*.

A static assessment of data security risk management will not work in most instances, given the rapid pace of change in this area. Be vigilant and adaptable in managing the security risk. Work with your colleagues in other departments to reduce risk where you can — and secure the best insurance your company can afford to protect against losses stemming from cyber-related perils. ▲

ENDNOTES

1. According to the April 2015 *Global Cyber Impact Report* sponsored by Aon Risk Services and conducted by Ponemon Institute LLC ("Aon-Ponemon Study"): "Despite the cyber risk, only 19 percent of respondents say their companies currently have cyber insurance coverage with an average limit of $13 million." *Id*. at 11
2. *See* https://www.travelers.com/business-insurance/cyber-security/technology/cyber-first.aspx.
3. No. 2:14 CV 170 TS (D.Utah), *Memorandum Decision and Order Denying Defendants' Motion for Partial Summary Judgment,* dated May 11, 2015. *See also* Joshua Gold, *Beware of Holes in Your Cyber Insurance Policies,* Agents of America, May 27, 2015.

4. *See* http://www.wsj.com/articles/how-the-sony-data-breach-signals-a-paradigm-shift-in-cybersecurity-1423540851

5. For example, it was noted in *Sony Employees' Data Breach Class Action to Proceed; Some Claims Dismissed*, Mealey's Cyber Tech & E-Commerce, June 18, 2015, that the Sony Pictures hack involved, among other things, "Guardians of Peace (GOP) [taking] control of Sony's network, displaying messages and a skeleton image. GOP also seized control of various Twitter accounts for Sony movies. Since then, GOP has made well-publicized releases of information related to various Sony movies and celebrities affiliated with the firm." Sony employees are suing, claiming that better security, firewalls and encryption technology should have been applied to minimize the risk of a hack. Accordingly, it is clear that the Sony Pictures hack implicates serious concerns beyond just the usual exposures involving health information, customer payment information and class action suits over credit monitoring. Good will, employee communications and business proprietary information are also vulnerable and often targeted.

6. *Hackers ground 1,400 passengers in attack on Polish airline LOT*, AFP World News, June 22, 2015.

7. *See* Joshua Gold, *D&O Insurance for Data Breaches,* Risk Management, April 2, 2014; Young Ha, *Executives Examine D&O Claim Trends, Cyber Exposure,* Insurance Journal, March 6, 2015. (reporting that "As a source of losses, or a type of D&O loss, [cyber perils are] obviously a new thing, and getting a tremendous amount of attention. The SEC has commented with increasing frequency about the need for directors to make sure that the company is prepared for attacks on their data.").

8. *See* Chip Phinney, *Data Security Breach Documents Sought in Home Depot Books-And-Records Suit*, Mondaq Business Briefing, June 22, 2015 (noting that "Home Depot was recently hit with a books-and-records suit in the Delaware Court of Chancery . . . relating to the giant retailer's data security breach last September" and that such actions are often precursors to derivative lawsuits).

9. Robert A. Bregman, *Cyber & Privacy Insurance Coverage Made Simple(r)*, IRMI Webinar, September 25, 2014 (explaining that "Unfortunately, the insurance policies written to cover cyber & privacy exposures are anything but simple. Adding to the confusion is the fact that insurers' forms lack standardization, which makes it especially difficult to compare the various programs").

10. *See* Aon-Ponemon Study, at 13–15 (surveying risk trends, exposures and cyber insurance).

11. *See* John B. Dickson, *6 Ways the Sony Hack Changes Everything*, Dark Reading, Mar. 11, 2015 (noting that "Sony Pictures experienced what many are calling the most devastating cyber attack to date, disrupting a movie release, knocking its corporate systems offline for weeks, threatening its distribution channels with terroristic threats of mass violence, and ultimately costing [a senior executive] her job").

12. *See* Aon-Ponemon Study at 14, (finding that 25 percent of policyholders indicated their cyber coverage insured "revenue losses" and 15 percent indicated that their coverage provided protection against "brand damage." Compare that to 52 percent of policyholders indicating they purchased coverage for "defense costs," 71 percent purchased coverage for "forensics and investigative costs," and 43 percent purchased coverage for "third-party liability").

13. *See* Joyce Famakinwa, *Cyber business interruption tool calculates foreseeable losses,* Business Insurance, June 2, 2015 (reporting on insurance industry offered calculator and coverage tool for projecting "maximum foreseeable loss to business income at multiple key locations in the case of a cyber attack").

14. Claims-made policies seem to be favored by the insurance industry in the context of cyber liability coverage. *See* Richard S. Betterley & Sandy Hauserman, *Cyber Endorsements for Traditional Insurance Policies,* Risk Report, International Risk Management Institute, Inc., May 2013, at 2 ("Liability coverage for data breaches is fairly standard, providing coverage for legal defense and settlements or judgments. This coverage is almost always written on a claims-made basis[.]").

15. *See* http://www.riskpro.us/FAQ.html#no-known-claims.

16. *See* Joshua Gold, *Fighting Back Against the Insurance Industry's "Restitution"/"No Covered Loss" Defenses,* Policyholder Advisor & Alert (June 2014) (setting forth certain cases rejecting insurance company breach of contract defenses to coverage).

17. *See* http://venturebeat.com/2015/06/11/what-the-columbia-lawsuit-really-means-for-cyber-insurance/.

18. *See*, e.g., Speech of SEC Commissioner Luis A. Aguilar, entitled "Board of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus" presented at the Cyber Risks and the Boardroom conference at the New York Stock Exchange, New York, NY, on June 10, 2014. Commissioner Aguilar notes, among other things, that:

> As an SEC Commissioner, the threats are a particular concern because of the widespread and severe impact that cyber-attacks could have on the integrity of the capital markets infrastructure and on public companies and investors.[13] The concern is not new. For example, in 2011, staff in the SEC's Division of Corporation Finance issued guidance to public companies regarding their disclosure obligations with respect to cybersecurity risks and cyber-incidents.[14] More recently, because of the escalation of cyber-attacks, I helped organize the Commission's March 26, 2014 roundtable to discuss the cyber-risks facing public companies and critical market participants like exchanges, broker-dealers, and transfer agents.[15]
>
> Today, I would like to focus my remarks on what boards of directors can, and should, do to ensure that their organizations are appropriately considering and addressing cyber-risks. Effective board oversight of management's efforts to address these issues is critical to preventing and effectively responding to successful cyber-attacks and, ultimately, to protecting companies and their consumers, as well as protecting investors and the integrity of the capital markets.

19. *See* http://venturebeat.com/2015/06/11/what-the-columbia-lawsuit-really-means-for-cyber-insurance/.

20. *ACE Provides Roadmap of Cyber Risk Evolution*, May 7, 2015, http://www.claimsjournal.com/news/national/2015/05/07/263249.htm. According to the ACE group of insurance companies, of the seven main data breach triggers, lost or stolen devices accounted for 20% of the total. More specifically, "ACE found that 70 percent of devices lost or stolen were laptops, 28 percent were memory devices and 2 percent were smartphones."

21. *See* Joshua Gold, *How to Protect Data in the Cloud*, Risk Management, March 6, 2013.

About Anderson Kill

Anderson Kill practices law in the areas of Insurance Recovery, Commercial Litigation, Environmental Law, Estates, Trusts and Tax Services, Corporate and Securities, Antitrust, Banking and Lending, Bankruptcy and Restructuring, Real Estate and Construction, Foreign Investment Recovery, Public Law, Government Affairs, Employment and Labor Law, Captive Insurance, Intellectual Property, Corporate Tax, Hospitality, and Health Reform. Recognized nationwide by Chambers USA for Client Service and Commercial Awareness, and best-known for its work in insurance recovery, the firm represents policyholders only in insurance coverage disputes — with no ties to insurance companies and has no conflicts of interest. Clients include Fortune 1000 companies, small and medium-sized businesses, governmental entities, and nonprofits as well as personal estates. Based in New York City, the firm also has offices in Ventura, CA, Philadelphia, PA, Stamford, CT, Washington, DC, Newark, NJ, and Burlington, VT.