ANDERSON KILL
CYBER INSURANCE
ALERT
September 2017

The Equifax Hack:

Cyber Intrusions Pose Special Risks for Corporate Managers — Making Insurance Coverage Essential

By Joshua Gold

From a risk management point of view, there are plenty of lessons to be learned from the recent data security compromise at Equifax.

1. **No one is immune from a cyber attack.** Whether you are an individual, public company, government authority, health care provider, utility, or law firm, someone wants in. The attack vectors are numerous and creative, thus cyber risk can never be entirely contained.
2. If you are an officer or director and sell stock during the throes of a breach (especially before public disclosure), **the timing will look bad to regulators, investors and the public** — even where purely coincidental.
3. **Boards and senior corporate officers will be increasingly second-guessed** for missing warning signs of cyber security weaknesses. In a somewhat ironic twist, however, a recent report about a hack of the SEC's computer systems is bringing into question whether the SEC had appropriately enhanced its security after the completion of a GAO cyber security assessment.
4. **The timing of cyber intrusion disclosure will always be scrutinized.** I have been on conference panels with state attorneys general and federal regulators who almost uniformly assert that a delay in reporting a breach that lasts more than 30 days typically raises a red flag with them. That is not to say they will not recognize extenuating circumstances, but it is a baseline that has significance to many who wield power when it comes to investigations and litigation.
5. **Policyholders can expect that their boards and managers will be increasingly raked over the coals for the robustness of their cyber security.** This will be especially true where the data to be secured either bears on health and safety, or pertains to individuals (e.g., customers, patients, employees, etc.).
6. We can also expect that, for public companies in particular, **special focus will be trained on the level of insurance protection corporate managers have secured** to protect the balance sheet of the corporate entity for both first-party losses and third-party claims.

ANDERSON KILL
1251 Avenue of the Americas
New York, NY 10020
(212) 278-1000

ANDERSON KILL
1760 Market Street, Suite 600
Philadelphia, PA 19103
(267) 216-2700

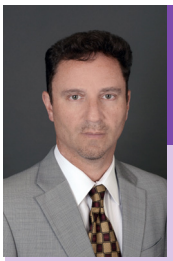
ANDERSON KILL
1055 Washington Boulevard, Suite 510
Stamford, CT 06901
(203) 388-7950

ANDERSON KILL
1717 Pennsylvania Avenue, Suite 200
Washington, DC 20006
(202) 416-6500

ANDERSON KILL
One Gateway Center, Suite 1510
Newark, NJ 07102
(973) 642-5858

ANDERSON KILL
Wells Fargo Building
355 South Grand Avenue
Los Angeles, CA 90071
(213) 943-1444

www.andersonkill.com



who's who

Joshua Gold is a shareholder in the New York office of Anderson Kill and chair of the firm's Cyber Insurance Recovery 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.
jgold@andersonkill.com
(212) 278-1886

Pre- and Post-Breach Cyber Peril Solutions

There are a number of things policyholders can do both pre-breach and post-breach to improve their station when it comes to cyber perils.

1. **At point of purchase, work with a skilled insurance broker** who can steer the company toward insurance products that provide comparatively better protection. There are lots of competing insurance products in the marketplace and they are not created equal. Smart shopping with careful broker guidance can mean the difference between meaningful insurance protection and an insurance policy that is not worth the paper it's printed on.
2. **Approach insurance applications carefully.** This means providing prudent responses to insurance applications after polling key internal departments within the policyholder's organization to make sure answers are correct. It also means pushing back against insurance application questions that are overly broad, vague or traps for the unwary.
3. **Provide proper and prompt notice of circumstances and claims.** When a cyber incident occurs, make sure to notice any and all potentially applicable insurance policies. Potential coverage for cyber losses and claims is not limited to insurance policies with the word "cyber" in them. We have secured insurance coverage for cyber-related claims under property, crime, E&O, D&O, commercial general liability and other first- and third-party insurance policies. The Equifax hack implicates a number of different insurance policy types that may provide coverage for claims against Equifax, potentially including losses to Equifax's own property and business operations. The hack may also implicate claims involving third-parties under their own insurance policies.
4. If a cyber claim is likely to focus attention on the board of directors or the officers, **consider whether a notice of circumstances to the company's D&O insurance tower (including Side A and excess policies) is the safest approach** despite the lack of an actual "claim" at the time. This can have implications for renewals, insurance application disclosures and possibly laser exclusions in the next year's D&O coverage.
5. **Be on guard for attempts to impose cyber exclusions at renewal time.** Directors and officers should take care to ensure that their D&O policy remains clear of cyber exclusions that have taken hold in other lines of coverage such as CGL and marine cargo insurance.

As many policyholders have already learned, insurance coverage can be a vital benefit when the sky is otherwise falling due to a serious cyber hack. It's imperative to ensure in advance that your coverage itself hasn't been hacked at by underwriters.