January 28, 2015

Weil

Alert
Cyber Security, Cyber Governance, and Cyber Insurance

Major Cyber Breaches Reveal Potential Cyber Insurance Coverage Gaps

By Joseph Verdesca, Paul Ferrillo, and Gabriel Gershowitz

News reports abound of cyber attacks and cyber security breaches. The damage resulting from such breaches can include loss or disclosure of confidential customer and employee data and mission critical intellectual property, destruction of business property, reputational injury, regulatory actions, fines and investigations, class action litigation, and loss of business, enterprise value, and market capitalization.

A comprehensive response to this growing threat must include a review of the degree to which the risks of cyber attack or breach are covered by insurance.[1] Particular attention should be paid to the following three contexts in which we have seen significant gaps in coverage of late:

- Cyber Exclusions in Directors' & Officers' Liability Insurance;
- War and Terrorism Exclusions in Cyber Insurance; and
- Coverage of Physical Loss Resulting from Cyber Attacks.

Cyber Exclusions in Directors' and Officers' Liability (D&O) Insurance

A cyber incident involving a company may have significant implications for its directors and officers. This is particularly true where the company has publicly-traded equity or debt securities, as such a cyber incident can adversely affect the holders of the company's securities, or where the company occupies a prominent or sensitive position from a governmental or regulatory perspective. For example, the degree to which a company's directors and management have complied with their fiduciary duties, taken appropriate precautions against cyber-related risks, and adequately disclosed such risks and related precautions may well be called into question in shareholder or creditor litigation or during a regulatory inquiry or investigation.

In seeking to mitigate the impact of cyber-related claims against a company's directors and officers (for example, where the company's share price drops following the disclosure of a cyber-related incident, and shareholder derivative claims are brought), one might first turn to the company's D&O insurance policy. However, we have seen several instances of existing policies (and proposed renewals of D&O insurance policies) containing exclusions of coverage for cyber-related matters, including for "cyber security breach" and "data breach". The existence of such exclusions could[2] eliminate

D&O insurance coverage for a particular cyber incident, thus leaving the company with only its cyber insurance coverage limits (if and to the extent it has them) to address the costs and liabilities suffered by the company directly, as well as the costs and liabilities incurred in the defense and settlement of any related shareholder complaint.

We encourage you to review carefully with your insurance and legal advisors the terms of your existing D&O insurance policy to ascertain whether the foregoing exclusion applies to your coverage.

War and Terrorism Exclusions in Cyber Insurance

Insurance policies routinely exclude coverage for losses resulting from acts of war or terrorism. Recent cyber-related incidents, particularly those involving or allegedly involving governmental or quasi-governmental actors or terrorist groups, raise questions of whether such incidents would fall within the scope of such exclusions. The globe-spanning nature and armchair execution of cyber threats, together with reports that certain cyber attacks have been conducted by or on behalf of governmental actors, distinguish the risks covered by cyber insurance from risks covered by other forms of insurance. A company purchasing cyber insurance expects coverage in the event of a cyber incident, irrespective of the identity of the perpetrator (including persons acting for or on behalf of other countries) and the reason for the cyber incident (including perpetrating acts of "cyber terror").

Cyber risks and cyber insurance are still evolving. In evaluating or purchasing cyber coverage, special attention must be given to exclusions for "terrorism", "war",[3] "government action",[4] and other terms having similar import. The presence of these types of precise formulations of such exclusions could eliminate coverage for a cyber incident, merely by virtue of who perpetrated the act, for what reason the act was perpetrated, and/or how the act or a person, group, or country allegedly involved in the act is characterized by a politician, governmental agency, or regulator. We urge you to keep this in mind and discuss with your insurance and legal advisors when assessing protection afforded by existing cyber insurance coverage or in negotiating new or renewal coverage.[5]

Coverage of Physical Loss Resulting from Cyber Attacks

Exclusions for cyber-related matters are found in many commercial general liability (CGL) insurance policies today, and such exclusions are being routinely included in CGL insurance renewals. Depending upon the formulation of such exclusions, the remainder of the policy language and the ongoing development of case law in this arena, coverage for losses from bodily injury, physical damage, pollution, or similar matters may not be available if arising from a cyber-related incident. Similarly, typical cyber insurance policies often expressly exclude coverage for such losses.[6] Examples of such losses could include damage to persons or property (including pollution) resulting from a cyber-based attack on oil, gas, electrical, and other infrastructure control systems,[7] personal injury resulting from a cyber-based shut-down of healthcare or emergency responder systems, and destruction of computer hardware (including servers) and other assets through a cyber-based attack.

As a result, unless its insurance program has been carefully constructed and modified as necessary as developments in the cyber arena emerge, a company may find itself without any insurance coverage for potentially material liability arising from cyber-related incidents, merely by virtue of the type of damage caused by such incident. One recent commentator noted, "[a]lthough the upstream, midstream and downstream energy markets are well-insured, many of these insurance policies contain exclusions for damages arising out of cyber attacks, malevolent viruses or malware. The end result is an ocean of insurance coverage, but barely a drop that would cover catastrophic damages arising from a cyber attack."[8]

In this age of cyber crime and cyber terrorism (and continued evolution of cyber insurance and cyber-related exceptions from non-cyber insurance policies), insureds would be well-advised to review with their

insurance and legal advisors their property and casualty and cyber insurance policies to see whether and how they would respond to physical loss in the face of any of a number of potential cyber-related incidents.

---

1. For a discussion of how insurance may be useful in mitigating cyber-related risk, please see "Cyber Security, Cyber Governance, and Cyber Insurance," available at http://blogs.law.harvard.edu/corpgov/2014/11/13/cyber-security-cyber-governance-and-cyber-insurance/.
2. A careful, case-by-case review of the precise policy wording is necessary to determine coverage availability.
3. For example, an "Acts of War" exclusion may provide that "This policy shall not cover the defense of any matter, or any loss, injury, damage, costs, expenses or other amounts … arising out of, based upon or attributable to any strike, lockout, disturbance or similar labor action, war, invasion, military action (whether war is declared or not), political disturbance, civil commotion, riot, martial law civil war, mutiny, popular or military uprising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against any of these events; whether or not any other cause or event contributed concurrently or in any sequence to any resulting loss, injury, damage, costs, expenses or other amounts…."
4. For example, a "Government Action" exclusion may provide that "This policy shall not cover the defense of any matter, or any loss, injury, damage, costs, expenses or other amounts … arising out of, based upon or attributable to any seizure, confiscation, nationalization, breach of security, use, misuse or destruction of a Computer System or Electronic Data by or on behalf of any governmental, military, enforcement or other public body or authority; whether or not any other cause or event contributed concurrently or in any sequence to any resulting loss, injury, damage, costs, expenses or other amounts…."
5. We note that express coverage of "cyber terrorism" is available from some insurers, but caution that the precise formulation of such coverage and how such wording interacts with the remainder of the policy requires careful review in order to avoid potential coverage surprises.
6. Certain cyber insurance policies are designed to provide cover for such losses in the case of a cyber-related incident excess of any coverage provided by a CGL policy. See, e.g., "Cyber Edge PC," available at http://www.aig.com/cyberedge-pc_3171_595334.html.
7. Admiral Rogers, head of the United States Cyber Command, has been quoted as saying "[w]e have seen instances where we're observing intrusions into industrial control systems…. What we think we are seeing is reconnaissance by many of those actors in an attempt to ensure they understand our systems, so that they can then, if they choose, exploit the vulnerability within those control systems…. There shouldn't be any doubt in our minds that there are nation states and groups out there that have the capability to … shut down or stall our ability to operate our basic infrastructure, whether it is generating power across this nation, or moving water and fuel." See "Cyberattackers have penetrated U.S. infrastructure systems – NSA chief," available at http://www.eenews.net/stories/1060009391.
8. See "Cyberattack Insurance Challenges Confront Energy Sector," available at http://www.law360.com/articles/591022/cyberattack-insurance-challenges-confront-energy-sector.

If you have questions concerning the contents of this issue, please speak to your regular contact at Weil, or to:

Joseph T. Verdesca (NY)	Bio Page	joseph.verdesca@weil.com	+1 212 310 8838
Paul A. Ferrillo (NY)	Bio Page	paul.ferrillo@weil.com	+1 212 310 8372
Gabriel Gershowitz (NY)	Bio Page	gabriel.gershowitz@weil.com	+1 212 310 8465