when global trade volumes are down, commodity price declines continue to batter emerging markets and central banks openly speculate as to what recourse is available if global growth rates further decline.

This is all cause for concern. Yet the global risk situation remains manageable. Executives need to have a clear-eyed view of the challenges of a less stable world and an openness to the new forms of risk management, including insurance, designed to meet these challenges. When they do, they will continue to contribute to a global economy that has brought better lives to millions of people around the world.

DIRECTORS AND OFFICERS MAY NEED TO RE-THINK COVERAGE IN A CYBER WORLD (1,076)

By: Daniel J. Healy

By 2016, it is no longer news that major data breaches can lead to lawsuits targeting directors and officers, sometimes personally. Allegations of improper management of corporate cyber risks form a basis for lawsuits that aim for the boardroom. In the wake of data breaches, shareholders have filed derivative suits, regulators have initiated enforcement proceedings, and management has been forced to defend their cyber-risk protocols. Even assuming the board acted properly – or at least defensibly – the investigation and defense of allegations can be a costly undertaking.

> Just in case directors and officers were unsure, in April 2016 Fitch Ratings reported*:
>
> "D&O-related exposures from cyber events arise through allegations that ineffective or negligent corporate governance and board oversight were contributing factors behind inadequate systems defenses and a breach that led to losses and/or a sharp decline in share value…"

The likelihood of suffering a cyber event has become nearly a given. Key steps in responsibly managing cyber risks include identifying, securing and pursuing insurance coverage. Such coverage ideally provides financial security for a growing risk.

A cyber policy alone may not offer adequate protection against shareholder suits. Directors and officers and errors and omissions policies arguably are more likely to provide the chief line of defense against such suits. General liability and cyber liability policies cover losses involving bodily injury, property damage, personal and advertising injury, and possibly damage to intangible property. They may exclude damage from providing services, from professional liability or from the loss of use of tangible property. They may not apply to shareholder derivative suits or investigations of management either. Additionally, they cover the corporation, not the individual directors and officers. Last, general and cyber liability policies may be exhausted before shareholder claims and government investigations are commenced. In sum, a review of existing policy language is an appropriate first step.

Additionally, the technological nature of cyber exposures has evolved rapidly and the resulting losses are not always the same. The losses stemming from the exposures vary. Cyber extortion seeks money, other hackers seek to steal the data itself, still others seek to destroy a corporation's data or functionality, and more radical hackers have taken over computer systems to vandalize the corporation's property, such as an oil pipeline that spans multiple countries. The monetary risks alone can be immense. The highly publicized Target breach included $150 million in initial response costs, $400 million in replacement credit cards, and an estimated $1 billion of ultimate costs. In many corporate hacking scenarios the corporation moves swiftly from the victim of a hack to the target of lawsuits. Policyholders need to be sure the losses they stand to suffer are contemplated in their coverage.

Management should, of course, minimize corporate exposures by implementing enterprise-wide procedures and standards applicable to cyber risks that cross corporate departments and real-world geography. Several federal agencies, including the Securities and Exchange Commission, the National Institute of Standards and Technology and Federal Trade Commission, have issued guidance for adopting measures. In addition to preventing some breaches, adopting good practices will also position a corporation to minimize loss after the inevitable, successful attack, at which time insurance coverage becomes vital.

Within the variety of losses, the liability that directors and officers may bear, or their corporation may bear through indemnity obligations, is a potentially large exposure. Directors and officers may need to look to more traditional E&O and D&O coverage, even for cyber-related losses. That means the exclusions and endorsements relating to cyber coverage, including the lack of such provisions, should be an important topic for boards to consider.

E&O policies typically cover losses from services provided to clients. D&O policies generally cover "wrongful acts" by management. Of course, cyber-related losses should not be specifically excluded, though they sometimes are. Additionally, the definitions of services, "wrongful acts" and other key grants of coverage should be broad enough to encompass the types of events that could lead to a data breach, whether due to an external hacker, internal employee conduct or so-called "social engineering." A surprising number of corporate managers and their boards are not aware of whether their D&O or E&O coverage specifically exclude cyber risks, and do not understand how cyber coverage works or what triggers it.

Key terms that often become important after claims are submitted include "claim," "wrongful act," and "misrepresentation." Among other terms, insurance companies often look to use these terms to narrow or decline their coverage

obligations. Questions policyholders should be asking prior to a claim arising include whether the definition of the types of "wrongful acts" covered under a D&O policy are defined broadly enough to encompass the board's decision-making process and representations made to the public about their corporation's cyber risks, policies and security.

Similarly, is a demand letter, subpoena or summons from a regulatory a "claim" under the terms of the applicable policy. Coverage for investigations can be extremely valuable, particularly as regulators have honed in on cyber issues in the past couple of years.

Conversely, any exclusions for alleged fraud should be narrow and, ideally, not exclude coverage for innocent misrepresentations. Recent case law has gone in different directions over whether misrepresentation needs to have been intended or not, or been subjective or objective, to be excluded, depending on the policy language. It may be crucial to have narrow language in such an exclusion if a corporation is making public disclosures about the online security measures that it has employed.

Additionally, exclusions relating to employment practices, bodily injury and personal/advertising injury ideally should not apply to data breaches that lead to such harm.

Similarly, the covered geographic area should include those locations where the company stores data, and perhaps extend globally, given the reach of the internet. Additionally, as many in-house counsel and board members know, D&O policies provide "Side-A only" coverage that should not be eroded by corporate losses. Given the high monetary exposure, it would be unfortunate to have no "Side-A only" coverage for a data breach due to exclusions.

Without making sure a policy contains the appropriate language, directors and officers risk finding out they have insufficient coverage after a loss. Recent case law suggests that coverage may pivot on the exact language of a policy, even under "traditional" policy language. Directors and officers need to be mindful of the coverage, or gaps in coverage, their corporation may have.

Taking stock now will greatly increase the chances of recovering insurance proceeds when they are needed, after a loss.

* http://www.businessinsurance.com/article/20160413/NEWS06/160419925/cyber-risks-fitch-ratings-chubb-ace-aig-xl-catlin-u-s-directors-and

NEW IRMI EXPERT COMMENTARY AVAILABLE

By Jack Gibson, CPCU, CRIS, ARM, President, International Risk Management Institute, Inc.

Assessing Risk and Cyber-Security (971)
Regardless of the goals of your company or organization, being successful depends on keeping assets secure. As a cyber-security expert, I make sure that digital assets are being kept safe from cyber-security threats and that this risk is managed in a cost-effective and efficient way. Read full article here

Touchdown! Analytics in College Football (1,404)
Hook 'em Horns! Roll Tide! O-H-I-O! T-R-O … J-A-N! USMA Rah Rah!, 1-2-3-4, 1-2-3-4, C-L-E-M-S-O-N! T-I-G-E-RRRR-S! Boomer Sooner! Go Irish Go! It's that exciting time of year again—college football season. College football is fun and a big money machine. Read why analytics play a huge role here

Little Known/Little Utilized Provisions of the CGL Policy (756)
If the truth be told, most people do not take the time or effort to read the insurance policies they purchase. They depend on their agents to identify the coverages that are required and to obtain them for their benefit. Even among the people who do take the time to read and analyze insurance policies, there are provisions in the commercial general liability (CGL) insurance policy that are relatively unknown and underutilized. Learn why the Declarations provision in the Conditions is so important here **ISN**