Why Your Company Should Review its Insurance Policies Now in Light of Tough New Cybersecurity Regulations

By: Brandy L. Worden

New York's new cybersecurity regulations just went into effect on March 1, 2017 and companies across the United States should take note. Inspired by the blockbuster proportion breaches that tanked stocks of massive corporations including several Fortune 100 companies, these regulations are recognized as the most stringent in civilian existence. As described by a statement released by Governor Cuomo, "these strong, first-in-the-nation protections will help ensure this industry has the necessary safeguards in place" to protect businesses and clients "from the serious economic harm caused by these devastating cyber-crimes."

As drafted, these rules seem to only apply to certain insurers, banks, money services businesses, regulated vital currency operators and their vendors. However, as detailed below, this should have your company on alert even if it is not in the financial services or insurance industries and even if it is not doing business in New York. These far-reaching regulations should also motivate your company to act now to prepare an insurance program to protect from the potential liability these regulations expose.

The Low Down on the Regulations

These extensive regulations contain 23 separate sections. Some key provisions of the new regulations require covered entities to do the following:

(1) Conduct a cybersecurity risk assessment and prepare cybersecurity program and written policy tailored to the company's individualized risks. The policy must be approved at a high level, for example, by a senior officer or board of directors and the cybersecurity program must be regularly audited and tested.

(2) Appoint a Chief Information Security Officer responsible for the cybersecurity program and policy that reports regularly about the integrity, security, policies, procedures, risks, and effectiveness of the cybersecurity program and of cybersecurity events.

(3) Require multifactor authentication for remote access of internal servers.

(4) Encrypt nonpublic information (includes personal information and other types of information) and regularly dispose of any nonpublic information no longer necessary for its business (unless required to be retained by law or disposal is not feasible).

(5) Prepare a written incident response plan that effectively responds to cybersecurity events and immediately provide notice to the Superintendent of the New York Department of Financial Services of any breaches where notice is required to be provided to any government body, self-regulatory agency or any other supervisory body or where there is a reasonable likelihood of material harm to the normal operations of the business.

(6) Annually file a statement with the New York Department of Financial Services certifying compliance with the regulations.

Why These Regulations Matter to Your Company

Understandably, you might think that if your company is not in the financial services or insurance industry or doing business in New York, that these regulations should not be relevant. Unfortunately, that could be a short-sided take on these regulations that could put your company at risk.

Laws struggle to keep up with technological advancements leaving courts in a position of interpreting what type of conduct a company should be liable for when a situation such as a data breach occurs. The impact of significant data breaches in recent history and the extensive regulations promulgated by New York could provide plaintiffs' attorneys with context in which to argue that your company should have done more to prevent a data breach, meaning more potential exposure for your company. What's more, regulation in one state often begets regulation in another state. California in particular is a state that has traditionally fought to lead the pack in consumer protection regulations and your company should be prepared for the potential promulgation of similar regulations in your backyard. *For more information on the prior California Attorney General's positions on data breach issues, please see the February 2016 California Data Breach Report* https://oag.ca.gov/breachreport2016.

Insurance Implications

These cybersecurity regulations create more paths to liability for your company. The best way to head off this liability, in addition to paying attention to business practices, is to arm your company with the right types and amounts of insurance to protect your business from potential staggering losses. These regulations open the window for hits on your D&O policies that you might not have expected and that might need to be adjusted to account for this additional potential exposure. For example, requiring approval of the cybersecurity policies by a senior officer and requiring companies certify compliance with regulations could result in a claim against that officer and trigger D&O coverage. However, the policy needs to be reviewed to ensure it does not contain exclusions for cyber-related liabilities.

Many standard CGL or D&O policies do not provide protection from the other types of losses incurred in data breaches. You should utilize professionals to take stock of your company's risk levels and assess the possibility of getting a separate cyber policy or review your company's cyber policy again now if it already has one in light of these new potential liabilities. Companies should also be assessing the insurance policies of their vendors to ensure they aren't left holding the bag for cyber-related liabilities the company intended the vendor to cover, but that the vendor failed to sufficiently insure for.

Note that the potential for substantial future tax credits exists for cyber insurance coverage by a bill introduced in the last congressional session for companies adopting the National Institute of Standards and Technology cyber security standards (H.R.6032 (114th)). While this bill was not enacted in the last session, commentators believe that it is likely it will reappear in the current congressional session.

For assistance reviewing your coverage, please contact managing partner, Jeff Dennis, Esq. based in the Newport Beach office (949.854.7000; jeff.dennis@ndlf.com).

ABOUT NEWMEYER & DILLION LLP

For more than 30 years, Newmeyer & Dillion has delivered creative and outstanding legal solutions and trial results for a wide array of clients. With over 70 attorneys practicing in all aspects of business, employment, real estate, construction and insurance law, Newmeyer & Dillion delivers legal services tailored to meet each client's needs. Headquartered in Newport Beach, California, with offices in Walnut Creek, California and Las Vegas, Nevada, Newmeyer & Dillion attorneys are recognized by The Best Lawyers in America©, and Super Lawyers as top tier and some of the best lawyers in California, and have been given Martindale-Hubbell Peer Review's AV Preeminent® highest rating.

For additional information, call 949.854.7000 or visit www.ndlf.com.