Media, Privacy & Beyond

DEVELOPMENTS AND INSIGHTS RELATED TO MEDIA, PRIVACY, AND THE PRACTICE OF LAW

PRESENTED BY

LATHROP & GAGE LLP

Target Data Breach and NIST Cybersecurity Framework Raise Tough Insurance Questions

By Emily R. Caron on February 18, 2014

Last week, the White House and the US National Institute of Standards and Technology (NIST) released the voluntary cybersecurity framework they have been working on for a year—the result of an Executive Order entitled, "Improving Critical Infrastructure Cybersecurity." The hope is that this new framework will eventually lead to a more robust cyber insurance market with lower premiums. While 85% of corporate executives named cyber attacks as their greatest risk in 2013, less than 20% of companies purchase cyber insurance. The NIST framework is a set of industry standards and best practices to help organizations manage cyber security risks. The 41-page document can be found here. The framework's focus is to measure and mitigate risk in the country's cyber infrastructure to protect airlines, roads and other vital aspects of the U.S. economy, but serves as a good model for any organization.

This is timely in light of the many data breaches that have taken place of late. For example, unless you've been living under a rock, you know that Target announced the theft of financial information, including credit and debit card information and imbedded PIN numbers, from as many as 110 million customers. Since announcing the breach in December, information continues to come to light, and none of it is good. For instance, the *New York Times* reported that Target was vulnerable to the cyber-attack because its systems were "astonishingly open—lacking the virtual walls and motion detectors found in secure networks." Hackers planted malicious code in early November, and it went undetected for weeks. Remarkably, Target did not find the breach on its own; the Secret Service discovered it during an unrelated investigation where agents had been tracking hackers overseas, and discovered common thread in a string of suspicious credit activity: payments made at Target.

As Target's investigation continued, in early February, it came to light that the hackers found their gateway into the virtual candy store of credit card numbers through, like any good heist in an action movie, the HVAC. Only, instead of slithering through air ducts, it appears that the hackers used credentials that were stolen from a heating and air conditioning subcontractor in Pennsylvania. Apparently, retailers will grant access computer networks to HVAC vendors to allow them to make changes and adjustments remotely to cut heating and cooling costs.

The breach carries with it a hefty price tag. The *Times* article reports that damages could exceed $18 billion. Along with that, nearly 70 class action lawsuits have been filed, and there is a public relations nightmare with the onslaught of negative publicity. Analysts estimate that Target's profit per share slumped 47 percent in the three months through January, the biggest quarterly decline since 2006. Earnings for the financial year slid 32 percent, making this the worst annual performance since at least 1987, according to projections compiled by Bloomberg.

Also, by the way, if you were thinking that you are in the clear if you haven't suffered any suspicious charges on your card—think again. Experts predict that this will be the primary driver of credit card fraud for the next 12 months.

Fortunately for Target, the organization appears to have a lot of insurance in place. Reports are stating that between Cyber coverage and Directors and Officers (D&O) coverage, it has $165 million in total limits, after self-insuring for the first $10 million. However, there is a big gap between $165 million and $18 billion.

Companies should take this opportunity to learn from Target's misfortune and ensure that they are adequately insured—particularly with cyber coverage, which can be tricky to navigate. For instance, organizations falling victim to a data breach will be looking for coverage for undertaking a forensic study to figure out what happened, who was harmed, notifying the people who were compromised, dealing with the claims from the banks who have to reissue millions of credit cards and deal with fraudulent charges, and lost income for the organization, itself, as well as public relations related expenses as a result of the breach.

Some cyber policies provide that an insurer will reimburse "reasonable and necessary legal expenses, public relations expenses, postage expenses and related advertising" incurred to comply with state or federal privacy legislation mandating customer notification in the event of a network security failure.

Does that include forensic expenses? Are forensic expenses "legal expenses?" Does that include the investigation of notifying who will require notification? (No small task when millions of customers are involved.) What if the data wasn't removed, but only copied — will provisions covering "costs incurred to replace, restore or recollect digital assets" provide any coverage? What about fines from the government or from the Payment Card Industry for lack of compliance? Are those covered?

What about business interruption? An example of what you might find in a cyber policy provides coverage for income loss and extra expense incurred during the period of restoration resulting directly from an interruption or service, provided the network security failure took place during the policy period. What if, as in most breaches, it takes several weeks or months for the breach to come to light, and you have entered into a new policy period? Does that mean there is no coverage?

Policies also impart an obligation on the part of the policy holder to use due diligence and take precautions to protect itself against the potential for losses. Some also exclude losses arising out of a failure to reasonably maintain, update or upgrade network operations security. Will the carrier take the position that the claim is excluded because security measures failed?

Often, cyber policies have sub-limits associated with different areas of coverage. Be mindful of this. You may have a $10 million policy that carries a $500,000 sub-limit for certain areas of coverage, which will barely scratch the surface of a large scale data breach. If you are interested in additional discussion about this issue, you can find that here and here.

These are just a handful of issues to evaluate when you are placing your cyber coverage. Always be proactive and work with insurance brokers and counsel who are well versed in the cyber insurance marketplace. It's a good idea to evaluate the track records of the carriers who provide this type of coverage. Seek a carrier who has a history of providing coverage, and not a carrier who is embroiled in coverage litigation denying claims that would appear to be covered based on the plain language of its policies and its marketing materials.

With cyber security issues becoming more wide-spread, and with the advent of the new NIST framework, the cyber insurance market will be evolving. How quickly? That remains to be seen.

Media, Privacy & Beyond
Lathrop & Gage LLP
155 North Wacker Drive
Suite 3050
Chicago, IL 60606-1787
T: 312.920.3302
F: 312.920.3301