CYBER RISKS & LIABILITIES NEWSLETTER

November/December 2015

IN THIS ISSUE

Controversial Cyber Security Bill Passes Senate

In October, the U.S. Senate passed a version of the Cybersecurity Information Sharing Act (CISA), a bill that encourages companies to share information about cyber attacks and data breaches with the federal government. The bill includes the most sweeping cyber security regulations ever put forth by the U.S. government, and it’s not without controversy. While supporters argue that the bill could help both businesses and the government minimize the impacts of cyber attacks, a number of consumer interest groups and tech companies remain critical of it.

Sharing Information and Reducing Liability

The proponents of CISA contend that information sharing is vital to cyber security. By encouraging companies to share information about cyber attacks, data breaches and other cyber threats with the Department of Homeland Security (DHS), they argue that both governmental agencies and companies will be alerted to vulnerabilities earlier, and, hopefully, can then devise solutions to mitigate the damage of a cyber attack.

Moreover, as a way of encouraging companies to share information, the bill includes provisions that would limit the liability of companies in handing over potentially sensitive information. That provision does come with some caveats, and it requires companies to make good-faith efforts to anonymize sensitive personal information that may be attached to the data before sending it to DHS.

Consumer Privacy and Gray Areas

Privacy is the biggest concern for the bill’s critics. Many say that the language in the bill is so vague that it gives companies carte blanche to hand over virtually all private customer data. That concern has even extended to a number of tech companies, like Apple and Dropbox, who have publicly opposed the bill, in part fearing customer backlash against companies that agree to hand over customer data to the federal government

Others are concerned that the language is vague about just how far liability protections extend. For instance, if a company recognizes a vulnerability and reports it—but does nothing to correct the vulnerability—it’s unclear whether or not the proposed law would leave that company liable in the event of a data breach.

Future Unknown

Before becoming a law, Congress will have to resolve the Senate version with the House version of the bill. Rest assured that as the law and your liabilities change, your trusted advisors at Baldwin Krystyn Sherman Partners will keep you up to date.

BALDWIN
KRYSTYN SHERMAN

Cyber Crime's Forgotten Victim—Your Company's Reputation

Even though companies are finally starting to dedicate resources to prepare for cyber attacks, it's possible that they may be overlooking a key exposure. While internal audits, hardware and software upgrades, and payouts to customers whose personal information has been exposed can be costly, those costs can quickly be dwarfed by the damage a cyber attack can do to a company's reputation.

The Dark Side of Social Media
Social media poses a huge threat to your company's reputation. In the event of a data breach, traditional media coverage, blog posts and consumer reaction to the breach will dominate discussion of your company's brand across social media platforms. Social media newsfeeds offer little to no distinction between legitimate news, biased reports, rumors and outright falsehoods, making the problem worse.

Additionally, social media is the perfect battleground for a competing interest to launch an attack on your brand. In fact, a white paper released by Hays suggests that the deliberate spread of false information about companies could be part of the next wave of cyber attacks launched by foreign governments.

Managing Your Reputation
In the wake of a cyber attack, it's important to have a social media strategy in place and ready to roll out, as well as a team dedicated to monitoring social media in order to dispel any rumors and clarify any falsehoods. It's also important to consider all avenues for mitigating your risk.

To learn more about your insurance options, contact your broker at Baldwin Krystyn Sherman Partners today and ask about "Coverage Insights: Reputational Risk Insurance."

HSB survey finds most businesses lack cyber security resources despite being hacked

According to a survey conducted by The Hartford Steam Boiler Inspection and Insurance Company (HSB), 70 percent of risk managers reported that their companies had been victims of at least one hacking incident in the previous year. In spite of that, 55 percent said that their companies weren't designating enough money or trained personnel to combating the growing cyber security threat.

Risk managers cited a number of strategies that they wanted to deploy in order to combat cyber threats, including intrusion detection and penetration testing as well as employee education. Cyber coverage also made gains, with 46 percent of risk managers saying they'd either purchased it for the first time or purchased additional coverage in the past year. Still, 36 percent of respondents said their businesses do not have any level of cyber coverage at all.

Cyber security workforce projected to be 1.5 million short by 2019

As cyber attacks become more frequent and companies work to tighten security, the demand for cyber security workers will skyrocket to 6 million by 2019, with a 1.5 million worker shortage projected. Both governmental officials and companies are scrambling to train the next generation of cyber security experts. Until the labor supply meets the skyrocketing demand, employers can expect to pay high salaries to their cyber security employees.

Comcast set to pay $33 million in data breach settlement

On Sept. 17, 2015, Comcast agreed to pay a $33 million settlement for a data breach that led to the publication of nearly 75,000 of its subscribers' unlisted telephone numbers. The terms of the deal include $25 million in penalties and more than $8 million in restitution to the affected customers. The penalty may seem severe, but many people thought Comcast's handling of the breach left much to be desired. The breach occurred over a period of nearly two and a half years, from July 2010 to December 2012, and Comcast failed to take immediate measures to protect customers whose data was made public as a result of the breach.

CYBERRISKS&LIABILITIES_
NEWSLETTER

Baldwin Krystyn Sherman Partners
4010 W. Boyscout Blvd., Suite 200
Tampa, FL 33607
813-984-3200
http://www.bks-partners.com/