By Joshua Sebold

Nobody wants to be the next Trendnet Inc. The Internet-based security camera company became the example of how not to manage consumers' privacy after the Federal Trade Commission alleged its lax security practices exposed hundreds of customers' private lives to public viewing over the Web. According to the complaint, a hacker exploited the security flaws last year and made public nearly 700 live camera feeds. Trendnet settled with the FTC in September, agreeing to establish a comprehensive information security program.

Companies in many industries say cyberattacks are growing exponentially, a complaint that has triggered a variety of responses from federal agencies and from Congress over the past year. Much of that action has focused on improving information-sharing about such attacks within industries and between industry and government - a practice that attorneys say is one of the best ways to prevent future data breaches.

A key part of any legislation, corporate lawyers say, is that it protect companies from liability over such information-sharing. Companies are concerned that the more they share information about data breaches, the more they open themselves up to privacy litigation from consumers and from the federal government. While that concern was a centerpiece of discussions in Congress earlier this year, public concerns about privacy fueled by Edward Snowden's exposure of the National Security Agency's PRISM program have pushed discussions in the other direction. Most recently, Sen. Dianne Feinstein, D-CA, has been working with Sen. Saxby Chambliss, R-GA, on a bill that participants in any information-sharing programs be protected from liability stemming from disclosing information about cyberattacks.

"It seems like everything has died on the vine since the Snowden NSA crisis," said Karen L. Stevenson, of counsel at Buchalter Nemer PC, about the efforts to pass legislation permitting information-sharing by companies have been hurt by widespread privacy concerns.

One of the first developments came in February, when President Barack Obama signed an executive order meant to increase collaboration and develop standards for cybersecurity in the telecommunications, finance and energy industries - those deemed part of the country's critical infrastructure. The order tasked the attorney general, Department of Homeland Security and Director of National Intelligence with creating collaborative purposes and may not be distributed, reproduced, modified, stored or transferred without written permission. Please click "Reprint" to order presentation-ready copies to distribute to clients or use in commercial marketing materials or for permission to post on a website.
participants by setting up a structure by which that sharing could legally occur. The bill was viewed to be industry-friendly, including relatively limited requirements of companies to protect customers’ personal information, yet shielding the companies from liability for sharing it with one another. Unlike the executive order, the bill wasn’t limited to critical infrastructure industries.

But after months of public debate over consumer privacy, Feinstein’s bill may have a better chance of engendering support from legislators concerned with the optics of information-sharing. Thus have industry groups renewed their calls for protection from liability. Three financial industry lobbying groups - the American Bankers Association, The Financial Services Roundtable, and the Securities Industry and Financial Markets Association Inc. - wrote a letter to the U.S. Senate Select Committee on Intelligence in mid-November urging it to pass legislation that will protect their members from litigation associated with the data breaches or related information-sharing.

"It’s called a zombie bill because it’s died a couple times and been resurrected," said Andrew D. Castricone, a partner at Gordon & Rees LLP, of the bill.

Ultimately, many companies - especially those in the energy and financial services sectors - believe cyberattacks are much more of a threat to consumers’ safety than is the loss of their privacy to the government or other companies.

James M. Aquilina, executive managing director at computer forensics and consulting firm Stroz Friedberg LLC and a former federal cybercrimes prosecutor, said energy companies and utilities are increasingly becoming the target of specialized cyberattacks. He said most utilities and energy companies rely on complex computer systems to control and monitor industrial processes, known as supervisory control and data acquisition (SCADA) systems.

"What is of growing concern in my view is in recent years there’s been this development of malicious code that is designed specifically to attack SCADA,” Aquilina said. "It gives hackers the ability to alter the operation of industrial systems.”

Financial institutions have similar concerns.

"Most major financial institutions have seen a tremendous uptick within their IT security systems,” Stevenson said. "It’s not unusual to see thousands if not tens of thousands of attempts per day at security breaches throughout their networks.”

Nathan D. Taylor, a partner at Morrison & Foerster LLP, said financial institutions are already sharing information about cyberattacks in accord with prior executive orders affecting their industry. They're primarily looking to Congress for further guidance and protection against liability and litigation.

Aquilina said utility and energy companies have yet to establish communication systems about cyberattacks.

"[The executive order] is really the first public step we’ve seen here for establishing a normative framework for sharing information about cyberthreats,” he said.

While company-side attorneys view legislation regarding information-sharing on cyberattacks to be a critical step, Stevenson said she isn’t optimistic such a law will make it on the books anytime soon.

"I don’t see a swift passage of the legislation that’s been proposed by Sen. Feinstein,” she said.

joshua_sebold@dailyjournal.com

Previous    Next