Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Retailers Face Pitfalls In Effort To Share Cyberthreat Info

By **Allison Grande**

Law360, New York (June 04, 2014, 3:38 PM ET) -- A recent initiative by Target Corp., J.C. Penney Co. Inc. and other retailers to promote the sharing of cyberthreat information could provide the companies with a valuable tool to guard against data breaches and resulting negligence claims, as long as they're careful to act on common threats and avoid sharing customer data, attorneys say.

On May 14, the Retailers Industry Leaders Association along with dozens of **top U.S. retailers launched** the Retail Cyber Intelligence Sharing Center, in an effort to provide participating industry members with more detailed threat data, advanced training, education and research resources to combat increasingly sophisticated and prevalent cybersecurity threats.

The centerpiece of the initiative will be an information sharing and analysis center, or ISAC, aimed at facilitating the sharing of data on emerging threats to network security among industry members and with public-sector stakeholders such as the U.S. Department of Homeland Security, U.S. Secret Service and FBI.

"This initiative is a very important one that every retailer should look to participate in, especially given the **recent high-profile attacks** aimed at the industry," Gerald Ferguson, the co-leader of BakerHostetler's privacy and data protection team, told Law360. "One of the biggest challenges that every industry faces in responding to cyberattacks is that the hacking community is already working cooperatively, so to the extent that retailers are defending themselves in isolation, they're allowing themselves to be divided and conquered."

But while working together will likely provide a boost to retailers' data security, attorneys still caution that companies need to be mindful of the legal and competitive risks that could stem from sharing information and responding to potential threats.

"The reality is that no information sharing is risk free," Ferguson said. "But the benefits of cyber-risk information sharing outweigh the risks as long as the sharing is done in a smart way, meaning that the data shared is really limited to the characteristics of the attack rather than extraneous information about particular lawsuits or damage that occurred to third parties."

Erin Nealy Cox, an executive managing director of the cybersecurity consulting firm Stroz Friedberg, said it has been helpful that the U.S. Department of Justice and Federal Trade Commission issued a **joint policy statement** in April reassuring companies that legitimate sharing of cybersecurity information would not raise any antitrust concerns. But despite the green light, attorneys warn that there are still pitfalls that companies need to consider before opening up their books.

“By sharing information, companies are admitting to others that they had a vulnerability, and human nature is to be wary of exposing one's own vulnerabilities,” Proskauer Rose LLP privacy and data security group head Kristen Mathews said.

One significant impediment to widespread data-swapping is the risk that the shared information will be used against retailers in regulatory probes and private lawsuits over future security intrusions, according to attorneys.

“When a major data breach occurs, companies often get sued, and to the extent that they shared information about past security practices and attacks with third parties, that information could be discoverable,” Ferguson said.

That possibility enhances the need for companies to share data carefully, stripping the data of any information that could identify an individual and limiting disclosures to generalized threats that other retailers would be able to identify in their own systems.

“For example, if they identify a piece of malware or notice a new attack vector that is being exploited by hackers but hasn't been widely reported yet and isn't being picked up by spam or malware filters, that would be helpful to share,” Mathews said.

The limitations can also help alleviate concerns over competitors gaining access to information about a certain company's security weaknesses.

“Retailers wouldn't want to share anything involving competitive strategies about a product line, but if your organization has seen some spearfishing attacks coming through or has identified a specific pattern or trend tied to attacks, that information can be shared,” said Matthew Meade, co-chair of Buchanan Ingersoll & Rooney PC's cybersecurity and data protection group.

BuckleySandler LLP attorney James Shreve suggested that retailers that decide to engage in information-sharing arrangements establish formal guidelines for sharing and run disclosures regarding “particularly dangerous threats” by counsel.

“Companies need to make sure that they are comfortable with the types of information that are going to be out there before they share that information,” he said.

Retailers can also land in hot water if fail to act on pertinent threat data that could have helped them avoid or reduce the damage from a subsequent attack, attorneys noted.

“If a company has access to information about potential security threats but is not looking at it or keeping on top of it, and is a member in name only, that can be used against it,” said Moore & Van Allen PLLC member Karin McGinnis.

Target is already facing these types of failure-to-act accusations in some of the dozens of suits that have been lodged since its December breach. Litigants have based the claims on allegations that the retailer received a white paper identifying the vulnerability that had been exploited before the breach occurred but neglected to patch the hole, McGinnis noted.

On the other hand, attorneys say participation in the retail ISAC could end up helping retailers in legal

fights if they stay on top of the threats and take steps to respond accordingly.

“If you are a retailer who is active in the organization and have a breach that was the result of a hacking method that wasn't raised at all, then that would open the door for the defense that the company was taking reasonable measures and no one foresaw it,” McGinnis said.

And even though liability risks abound — a shortcoming that can only be addressed by Congress, which has so far **failed to act** — attorneys noted that ISACs already being used by the banking, real estate, health and several other industries have been operating without incident for years.

“Hospital organizations have been sharing information about risks related to that may affect implantable devices for years, and a lot of good has come out of that,” said Kenneth Rashbaum, the head of the privacy and cybersecurity practice at Barton LLP. “If this manner of information-sharing can be done in a way that doesn't expose personal data or specific access points that could provide a blueprint to systems, it can be very beneficial.”

--Editing by Elizabeth Bowen and Emily Kokoll.