U.S. Pressures Companies to Report Cybercrime

RICHARD LARDNER,Associated Press

WASHINGTON (AP) — Hackers broke into computers at hotel giant Wyndham Worldwide Corp. three times in two years and stole credit card information belonging to hundreds of thousands of customers. Wyndham didn't report the break-in in corporate filings, even though the U.S. Securities and Exchange Commission regulatory agency wants companies to inform investors of cybercrimes.

Amid whispers of sensational online break-ins resulting in millions of dollars in losses, it remains remarkably difficult to identify corporate victims of cybercrimes. Companies are afraid that going public would damage their reputations, sink stock prices or spark lawsuits.

The chairman of the Senate Commerce, Science and Transportation Committee, Democratic Sen. Jay Rockefeller, is adding a provision to cybersecurity legislation that would strengthen the reporting requirement. The SEC's guidance issued in October is not mandatory. It was intended to update for the digital age a requirement that companies report "material risks" that investors want to know.

Rockefeller's measure would direct the SEC's five commissioners to make clear when companies must disclose cyber breaches and spell out steps they are taking to protect their computer networks from electronic intrusions.

The SEC recently challenged Internet retailer Amazon's decision to omit from its 2011 annual report references to the online theft of customer data held by Zappos, an online shoe company owned by Amazon. Amazon eventually agreed to modify the statement slightly, according to correspondence between the company and the SEC. But the company still argued that the Zappos attack was not covered by the commission's cybersecurity guidance because it had no material impact on Amazon's business.

Cybercrime is rampant and not confined to the United States. The head of Britain's domestic spy agency said this week that cybersecurity ranks alongside terrorism as one of the United Kingdom's most pressing security challenges. In one recent case, an unspecified, London-listed company hit by a cyberattack incurred revenue losses of $1.2 billion, MI5 Director General Jonathan Evans said in rare public remarks in London. He did not identify the company or say which country was behind the attack. The U.S. has said China and Russia are the governments most frequently engaged in such hacking.

"What is at stake is not just our government secrets but also the safety and security of our infrastructure, the intellectual property that underpins our future prosperity, and the commercially sensitive information that is the lifeblood of our companies and corporations," Evans said.

Research by a cybersecurity expert shows dozens of Fortune 500 companies have lost a wide range of valuable information to cybercrimes, including intellectual property, bank account credentials, restricted data about patients of pharmaceutical companies and internal legal records.

Rodney Joffe of Neustar, an Internet infrastructure management company in Virginia, monitors networks used by online criminal groups and traces the origin of stolen information. He found evidence that 162 out 168 companies in the manufacturing, chemical and transportation sectors had been compromised. The names of the companies are being kept confidential for proprietary reasons, he said.

"No one is safe. Everyone is compromised," said Joffe, Neustar's senior technologist. "When people tell you, 'We are protected as a company,' they are really fooling themselves."

The SEC isn't tracking how many companies comply with its cybersecurity guidance. But publicly traded companies historically have resisted supplying information about cyber incidents because it highlights their weak spots, said Peter Toren, a former federal prosecutor with the Justice Department's computer crime division.

"It just doesn't look good," Toren said.

The breach of Wyndham's computers was described in a Federal Trade Commission lawsuit filed this week against the company and three subsidiaries for alleged security failures that led to the three data breaches between April 2008 and January 2010. The failures caused "the export of hundreds of thousands of consumers' payment card account information to an Internet domain address registered in Russia" and millions of dollars in fraudulent charges on consumers' accounts, the FTC said.

Wyndham didn't mention the break-ins in its 2011 annual report or prior securities filings, according to an Associated Press review of the records.

Wyndham's 2011 annual report said the "hospitality industry is under increasing attack by cyber-criminals in the U.S. and other jurisdictions in which we operate" and noted that it was involved in "claims relating to information security and data privacy." Wyndham spent $13 million more on security improvements and expects to spend as much as $100 million in 2012 to guard against "the increasingly aggressive global threat from cyber-criminals," according to the report.

Wyndham said in an emailed statement to The Associated Press that it "fully complied with SEC regulations in regards to the disclosure of material events." In the statement, Wyndham said the incidents were "previously reported," an apparent reference to notices to consumers that were published on the company's website. The company also said the FTC's claims were without merit.

Network infrastructure company Verisign reported in late October, just a few weeks after the SEC issued the guidance, that there had been several successful

cyberattacks against its corporate networks in 2010. In the filing, Verisign said the company's management had not been informed of the attacks until September 2011.

LinkedIn, the online networking service, publicly announced on June 12 the online theft of 6.5 million user passwords. It said the announcement complies with its obligations to the SEC, but it has yet to file a report about the incident with the commission.

The new SEC guidance puts pressure on companies to decide whether to disclose a breach or keep it secret, said Jody Westby of Global Cyber Risk, a consulting firm. But she said the demand for information amounts to locking the door after the house has been robbed.

"The SEC would have done better to require all public companies to say whether they've taken actions to implement a security program," Westby said.

—

Associated Press researcher Julie Reed contributed to this report.

—

Online:

SEC disclosure guidance: http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm *[1]*

Source URL (retrieved on *09/01/2014 - 3:39pm*):
http://www.chem.info/news/2012/06/us-pressures-companies-report-cybercrime

Links:
[1] http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm