MSNBC.com, Scores of U.S. firms keep quiet about cyber-attacks (6.13.12)

NEW YORK (Reuters) - Scores of U.S. companies have not disclosed breaches of their computer systems, even though eight months have passed since U.S. securities regulators issued guidelines on disclosing cyber attacks, according to leading security experts.

Calling for more rigorous rules and enforcement, these experts told the Reuters Global Media and Technology Summit in New York they know of many cyber intrusions, thefts and other digital security issues that were kept quiet.

"There have been lots of breaches in every industry that have never been publicized," said Shawn Henry, the FBI's former top cyber cop, who joined a new cyber security company, CrowdStrike, in April.

Henry said the FBI was working on 2,000 active cyber cases when he retired from the agency in March. "There's only a handful of cases that anybody has ever heard about," he said.

U.S. government officials and cybersecurity consultants have been raising alarms about the growing sophistication of attacks on private and government computer networks.

The U.S. Securities and Exchange Commission issued guidance on October 13 that outlined how and when companies should report hacking incidents and cybersecurity risk. The guidance did not establish new rules, and many experts say it lacks the teeth to compel heightened reporting.

Some companies do not disclose cyber breaches because they feel they were not material, said Dmitri Alperovitch, founder and chief technology officer of CrowdStrike. He said he knew of a publicly traded defense contractor that lost intellectual property (IP) to China because of a cyber intrusion.

."The justification they used for not announcing is that they only do business with the U.S. government and it doesn't really matter that the Chinese stole all their IP because the U.S. government will never buy from China, so it wasn't really material to them," said Alperovitch, who declined to name the company.

MOST INTRUSIONS NOT DISCLOSED

The U.S. Office of Management and Budget said in March that a total of 107,655 security incidents were reported in fiscal 2011 by federal, state and local governments, commercial enterprises, U.S. citizens and international cyber organizations. Federal agencies are required to report such incidents, but corporate reports are voluntary.

Jeff Moss, a highly regarded expert on hacking who advises the U.S. Department of Homeland Security, said Washington should at least require companies to report breaches to the government - as Japan does - even if they do not make a public disclosure.

The U.S. government could keep the data confidential and use it to expand its understanding of attack techniques, said Moss, the chief security officer of ICANN, a nonprofit group that manages some of the key infrastructure of the Internet.

Henry and other top U.S. officials have underscored the severity of cyber threats by citing a case in which one publicly traded company lost $1 billion of intellectual property in a single intrusion over a weekend.

Henry declined to identify the company, but said many corporations were unaware that their networks had been breached until FBI agents notified them that they discovered proprietary, company-specific data outside their networks.

The former FBI official said it would be helpful to clarify the SEC guidance and provide more specifics to companies. Congress is also examining ways to ensure better reporting of cyber threats.

A Reuters review last winter of more than 2,000 SEC filings that mentioned cyber risks found that some companies revealed significant new information about hacking incidents, but the vast majority merely described a general risk of cyber incidents. Some defense companies and other firms known to have suffered computer breaches did not mention the incidents in their filings at all.

LinkedIn Corp, a social network for job seekers and professionals, last week became the latest high-profile company to be hacked. It said it was working with the FBI to investigate the loss of millions of member passwords, but has not submitted any SEC filing on the matter.

LinkedIn spokesman Hani Durzy said the company had complied with SEC requirements, and had been giving members and the public "ongoing disclosures" and updates on its corporate blog.

COMPANIES ARGUE THAT BREACHES ARE NOT MATERIAL

.Tom Kellermann, vice president for cybersecurity at Trend Micro, the world's third-largest maker of antivirus software, said it was imperative for auditors and boards of public companies to get more involved with cybersecurity efforts.

He cited a survey of 1,000 companies last year by Science Applications International Corp that showed 52 percent failed to report and remediate network breaches.

Kellermann said the SEC should start holding companies accountable for their failure to disclose. "There needs to be a precedent set," he said, adding that the SEC should require minimum "standards of care," including mandatory cybersecurity risk assessments and timetables for resolving issues detected.

Enrique Salem, chief executive of Symantec Corp, the world's largest maker of security software, said the SEC guidance had sparked increased interest among corporate boards and audit committees, but disclosure rates were still low.

"Shareholders have a right to know if their investment is somewhat at a new risk, or if they've lost intellectual property," Salem said.

Symantec itself did not disclose a 2006 breach until this year, when hackers revealed they had obtained the proprietary source code, or blueprints, to several key products including older versions of Norton antivirus software.

Symantec said while it had investigated the breach in 2006, it did not know about the theft of the code at the time.

"We have disclosed everything," Salem said.

(Additional reporting by Jim Finkle in Boston; Editing by Matthew Lewis)