TheStreet

September 26, 2016

Federal and State Regulations for Companies Disclosing Data Breaches Remain Murky

When companies are breached, they are required by the SEC and state regulatory agencies, but the rules are vague and fraught with loopholes

By Ellen Chang

The breach at Yahoo (YHOO) is likely the largest hacking incident to date to occur, as the company confirmed last week that it affected 500 million users in 2014, but other infiltrations have remained under the radar.

When companies are breached, they are required by the SEC and state regulatory agencies to disclose the incident, but the rules are vague and fraught with loopholes. Each state has its own notification requirements while the SEC says the hacking incidents need to be materially relevant to be declared.

Determining how soon a company needs to disclose their hacking incident is complicated as some companies work first with law enforcement to determine the breadth of the infiltration and what information was stolen. Some experts believe the regulations need to be stricter so the public can be informed sooner that their personal information, often containing financial information such as credit card data, was stolen.

> "Even if the hackers only obtained limited information, they just made it easier for someone else to get more information," [Brian] Mahany said. "Drawing the line has to be a common sense approach."

In Yahoo's case, the company confirmed two years after the fact that users were affected by a state-sponsored actor who was able to infiltrate their network and that they are working with law enforcement. The company did not name the country but said personal details that were stolen included names, telephone numbers,

Continued on next page

email address, dates of birth and hashed passwords. In some instances, encrypted or unencrypted security questions and answers were also breached.

Disclosure is convoluted, because the first priority for many companies is to protect their reputation, said Chris Roberts, chief security architect at Acalvio, a Santa Clara, Calif.-based provider of advanced threat detection and defense solutions. On the other hand, it is not always cut-and-dried for a company to determine the amount of the loss.

"Is it really 'lost' if you can't find it out in the Darknet for sale?," he said. "Is it 'lost' if you have no trace of it leaving? Is it lost and do we have to disclose if we can't actually work out what happened? Disclosure is a mess, and that's putting it nicely. Lawyers are involved, and they care less about the 'normal human' and simply have a duty to protect the corporation. It's as simple as that."

Repercussions for companies failing to disclose breaches in a timely manner and update their software to prevent another intrusion can result in significant fines. New York Attorney General Eric Schneiderman fined the Trump International Hotels Management $50,000 on September 23 for breaches of 70,000 credit card numbers. The settlement stems from breaches that started in 2015.

"It is vital in this digital age that companies take all precautions to ensure that consumer information is protected, and that if a data breach occurs, it is reported promptly to our office, in accordance with state law," Schneiderman said in a statement.

Schneiderman's office said the company was informed as early as June 2015 that "multiple properties had been infiltrated with malware designed to steal credit card numbers and that banks had analyzed multiple fraudulent transactions and identified THC as a common point of purchase, Trump Hotel Collection did not provide notice to its customers until close to four months later, on September 25, 2015, when it placed a notice on its website about the data security breach. This delay violated New York's General Business Law § 899-aa which requires notice to consumers "in the most expedient time possible and without unreasonable delay."

SEC AND STATE DISCLOSURE REGULATIONS VARIES

Although the Securities and Exchange Commission has regulations for dealing with cyber attacks, their stance depends on the severity and frequency of the incidents, said Denver Edwards, a partner at the law firm of Bressler, Amery & Ross in New York and a former attorney with the SEC.

"Cyber is a 'relatively' new phenomenon and the SEC appears to be trying to fit regulation of cyber incidents into its existing regulations and Regulation S-K Item 503(c) discusses risk factors," he said.

The view of the SEC is that if cyber incidents are among the "most significant factors to make an investment risky or speculative, then disclosure is required," Edwards said. The other issues which have to be evaluated include the probability of the incident recurring, qualitative and quantitative consequences, costs and what assets are impacted.

Regulations which force a company to disclose every intrusion, "regardless of scale, may not be effective," he said.

The SEC focuses on whether a hacking incident is material to a company and this standard of disclosure by public companies has "worked well because it's able to adapt to the context such as circumstances, times and changing business conditions," Edwards said.

While the SEC began ramping up its reporting rules in 2013, there remain several loopholes in their current regulations on when a company needs to disclose an incident, said Brian Mahany, founder of Mahany Law in Milwaukee.

"There isn't much guidance for when a company must report,"

he said. “Certainly, if a hacker accesses tens of thousands of customer records, the event is reportable. Similarly, every time a worker gets an email suspected of containing malware, there is no duty to report. But what about the things which happen in between?”

Each of the government agencies such as the Office of the Comptroller of the Currency also have different regulations on when a company must disclose a hacking incident, depending on whether a company is a federal contractor and other issues.

“The problem is that there is a wide range of what is acceptable for reporting and it is a grey area,” he said.

In cases such as JPMorgan Chase, the companies “clearly had an obligation to report” because the attack jeopardized 83 million accounts, Mahany said. The attack occurred in July 2014, but was not reported until September 2014.

Customers should have the right to know immediately about a breach and not wait for a company to investigate the intent of the hackers, he said.

“Even if the hackers only obtained limited information, they just made it easier for someone else to get more information,” Mahany said. “Drawing the line has to be a common sense approach.”

Each state has set up its own regulations on when a company needs to disclose a breach and the agencies are all “playing catch up, but they should have seen this coming a long time ago,” Mahany said. Currently, 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have security breach notification laws and their definitions are “all over the place,” he said, based on data from the National Conference of State Legislatures.

WHY COMPANIES FAIL TO REPORT IMMEDIATELY

Since companies are often in a crisis management mode after a data breach, their “knee-jerk reaction is often to try and protect corporate reputation by maintaining strict secrecy over the breach,” said Brian Hussey, global director of incident response and readiness at Trustwave, a Chicago-based information security company. Determining the right timing to reveal a hack can be a tricky issue.

“If a company releases information before they have investigated the incident with qualified forensic experts, then they risk appearing clueless,” he said. “If they wait too long, they may appear as if they were hiding information. Generally, the best advice is to disclose information in stages, only release what is necessary and relevant to the affected communities and show that you are proactively investigating the incident.”

Businesses often adopt a reluctant stance on disclosing the incident, said Peter Toren, a partner who specializes in intellectual property and data protection at Weisbrod Matteis & Copley, a Washington, D.C. law firm and a former Department of Justice prosecutor with the intellectual property and computer crimes divisions.

“Companies who have become victims feel that they look bad to their shareholders and their competitors and unless there is some motivating factor, the number of cases is vastly underreported unless they are mandated by SEC or state regulations,” he said. “They will just live with it and go forward.”

Since many breaching incidents are unlikely to affect a company’s profit and the duty to report the incident to shareholders could potentially reveal trade secrets or intellectual property, companies have an “inherent bias against reporting,” Toren said. “What materially impacts a company is not always clear.” The regulations need improvement because it is “definitely a gray area,” he said.

Consumers often do not learn about major hacking incidents immediately because they are not advertised as broadly as they have been in the past, partly because companies have

improved their strategies on preventing them, said Nathan Wenzler, principal security architect at AsTech Consulting, a San Francisco-based security consulting company.

“There are still a lot of reports of hacking incidents such as the recent Dropbox and Brazzers attacks in the past couple of months, but I believe we’ve simply reached a point of media saturation with them,” he said.

Consumers must understand the severity of these breaches and companies should explain the extent of the attack better, Wenzler said.

“When the average user doesn’t feel like it affects them, these news events can sometimes be brushed off as not being a big deal,” he said. “Users don’t understand what the problem is and so they don’t take it as seriously as they should. It’s one of the reasons that many criminals have been able to get away with the theft of so much financial information and use it reliably and for long periods of time for monetary gain.” ■