

Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit www.djreprints.com

See a sample reprint in PDF format.

Order a reprint of this article now

THE WALL STREET JOURNAL.

WSJ.com

TECHNOLOGY | JUNE 17, 2011

Firms Adjust to Hacks

Armed With Crisis Plans, Companies More Readily Disclose Computer-Security Incidents

By BEN WORTHEN And ANTON TROIANOVSKI

When email-marketing firm Epsilon Data Management discovered in March that hackers had stolen consumer email addresses it maintains for major banks and retailers, Chief Executive Bryan Kennedy faced a choice: to disclose the breach or keep it under wraps.

Epsilon, a unit of Alliance Data Systems Corp. that runs email-based promotions and marketing campaigns on behalf of other companies, wasn't legally obligated to disclose the incident, as the data that were hacked weren't the type that triggered notification laws.

Such notification laws vary by state, but a breach typically has to involve credit-card numbers, Social-Security numbers or medical data before the laws apply.

"People recognize that these things happen," said Mr. Kennedy, so coming clean was an easy decision for him.

Year of the Breach

Epsilon : customer email addresses stolen March 31; disclosed April 1

RSA: security tokens compromised in March; disclosed March 17

Citigroup: credit-card numbers stolen May 10; disclosed June 9

Sony: customer data stolen April 18-20; disclosed April 26

Lockheed Martin: attacked May 21; disclosed May 28

In the 48 hours after the breach, Epsilon assembled a crisis team. It fell back on a breach-response plan it had previously developed, informing clients such as Target Corp. and J.P. Morgan Chase & Co. about the hack and advising them on what language to use when they notified affected individuals.

Epsilon then issued its own press release "to give our clients some air cover," Mr. Kennedy said. "It was clear that the most pragmatic approach was to get out in front of this."

How Epsilon handled to the breach is representative of how companies are shifting their responses to hacking incidents.

In the past, companies were typically caught off guard when a breach occurred and responses were often flat-footed, requiring updates and further clarifications to concerned customers.

Now an industry of experts—including lawyers, public-relations specialists and forensic

investigators—has emerged to help companies determine what to disclose and how to reassure victims. Executives outside the computer room are also more aware of the threat posed by hacking, leading companies to formulate breach-response plans before an incident ever occurs.

The shift comes as hacking intrusions become more commonplace and experience shows that revealing an incident won't necessarily cause lasting damage to a brand.

In fact, if a breach is handled well, "customer loyalty and your brand can actually improve," said Lori Nugent, an attorney who specializes in breaches at Wilson Elser Moskowitz Edelman & Dicker LLP.

Among the companies that have openly discussed having their systems compromised are Google Inc., which disclosed that hackers traced to China had stolen some of its intellectual property in early 2010, and EMC Corp.'s RSA security unit, which in April outlined how a hacker had broken into its systems and stolen information related to the security tools it sells.

This week, Citigroup Inc. said hackers had stolen nearly twice as many credit-card numbers as previously thought, while payroll services firm Automatic Data Processing Inc. said one of its systems had been breached.

These and other high-profile hacking attacks are changing the way the public perceives the incidents. "Breaches are increasingly viewed less as a weakness on the part of the company and more as the sophistication and relentlessness on the part of the hackers," said Michael Fox, who specializes in data-breach response at ICR Inc., a communications firm. "There's not as much of a stigma attached."

While a breach often results in fines and other costs, customers don't tend to flee. Sales at TJX Cos. Inc., the parent of TJ Maxx and other stores, climbed 7% in the fiscal year following its disclosure in January 2007 that hackers stole as many as 94 million credit- and debit-card numbers.

Companies still mishandle hacking incidents, of course. Sony Corp.'s PlayStation gaming network was unavailable for several days before the company disclosed in April it went offline as the result of a breach that compromised data belonging to 100 million people. Even then the company wasn't able to say conclusively whether credit-card numbers had been stolen.

That didn't go over well with David Weekly, a 32-year-old entrepreneur in Redwood City, Calif., who said he has had his account information compromised at least twice recently—first in December during a security breach at blog publisher Gawker Media and then with Sony.

While Sony waited days to inform its users of the breach, Gawker quickly alerted customers that passwords stored with the site might be compromised. Mr. Weekly praised Gawker's quick apology but said Sony took too long a time to notify him of what happened, and he still doesn't know for sure which of his data may have become available.

"The more annoying thing to me is that Sony has continued to be very tight-lipped about what information of mine is out there in the wild now," he said.

Sony has offered credit monitoring, identity-theft insurance and free games to those affected by the breach, and it has said that 90% of customers have resumed using its gaming network.

"We take each of our customers' concerns seriously, and we're working hard to make sure their questions are answered as soon as possible," a Sony spokesman said.

To mollify customers, companies are increasingly communicating exactly what happened in a breach and what risks are involved.

Automated Data Processing on Wednesday revealed a breach in its benefits-administration business, even though ADP said the breach was believed to have affected only one of its thousands of clients and occurred on a platform that is no longer being sold by its benefits business. A spokesman declined to comment.

Related

- Long Wait for RSA Security Tokens
- Citi Takes Heat Over Hack Attack
- Citigroup Says Hacking Affected 360,000 Cards
- Payroll Services Firm ADP Investigates Online Breach
- Citi Asked to Explain Data Breach (06/14/2011)
- Senate Website Gets Hacked (06/14/2011)
- Turkey Arrests Alleged Hackers (06/14/2011)
- IMF Mum on Details of Network Cyberattack (06/13/2011)
- Citi Defends Delay in Disclosing Hacking (06/13/2011)
- Spain Arrests Three in Sony Site Attack (06/11/2011)
- Survey: Breaches Cost Firms \$7.2 Million Per Incident (06/09/2011)
- Hackers Say They Hit a Sony Unit Network (06/07/2011)
- Security 'Tokens' Take Hit (06/07/2011)

Citigroup, meanwhile, disclosed the type of information the thief stole—credit-card numbers, names and email addresses—but also said the hacker didn't access Social-Security numbers or dates of birth and that the stolen data wouldn't be enough to execute credit-card fraud.

On Wednesday, the company provided the precise number of affected accounts—360,069—and even included a state-by-state breakdown of where victims lived.

Citigroup faced criticism for waiting as long as three weeks to notify affected customers, but breach experts said it is appropriate to take time to learn the true scope of an incident. A Citigroup spokesman said it is taking additional steps to protect against fraud, including monitoring affected accounts for suspicious activity.

At Epsilon, Mr. Kennedy, the CEO, doesn't expect any lasting damage from the March breach, which affected millions of people. The company, which sends more than 40 billion emails a year, said that about 2% of its customers were affected by the hacking incident. The company declined to provide further information on the breach.

"Our clients have stood by us, and we don't expect to see many changes there," Mr. Kennedy said.

—Randall Smith contributed to this article.

Write to Ben Worthen at ben.worthen@wsj.com