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

Hacking Attacks Highlight Importance Of Preparation

Law360, New York (February 19, 2013, 3:06 PM ET) -- Hacking attacks on major U.S. media properties appear to be on the increase. Over the past few weeks, The New York Times, The Wall Street Journal and other media outlets have reported sophisticated attacks on their computer systems. And social media giant Twitter recently disclosed attacks that led to the compromise of 250,000 account passwords. Although those passwords were reportedly hashed and salted, this increase in hacker activity raises significant concerns for just about any company with an online presence.

It is too early to know whether we are on the leading edge of a wave of attacks like we saw from Anonymous in 2011, or whether media and technology companies are being specifically targeted. What we do know is that sophisticated attackers, whether driven by criminal motives, corporate espionage or other reasons, are ever present, and organizations that collect and maintain user data or proprietary corporate information must be ever vigilant. The compromise of such data not only poses direct harm to users and companies, but also risks undermining user confidence in online commercial activities as well as inviting more aggressive regulation of these activities.

Data breaches of this type can be costly to a company's reputation and its bottom line, raising the specter of class actions and civil lawsuits, and myriad other costs. Yet companies that take the straightforward steps below can significantly mitigate such risks:

1) Ensure data breach incident response plans are in order.

Preparing for and responding to a data breach requires a coordinated approach that integrates litigation defense, regulatory, insurance and public relations. With an effective data breach plan, a company is better able to move past such situations quickly and efficiently, with minimal impact to its business.

2) Confirm that the company's insurance provides the key coverages needed for cyber exposures.

Data breaches can result in customer notification costs, forensic expenses, crisis communication costs, regulatory investigations, civil actions, credit card brand investigations and other reputational costs. A 2012 Ponemon study estimates that the average cost of a data breach to an organization is $5.5 million. Cyber insurance provides coverage for many of these costs, but the risks and the available coverages are rapidly evolving and should be reviewed periodically to ensure market developments are addressed. Companies should also review their first-party network/business interruption coverage in the event that a data breach or other system failure results in a significant network shutdown.

3) Confirm data retention policies are being implemented and that they have been updated to reflect the types of data collected and stored.

In general, the Federal Trade Commission requires that personal information (and data linked to personal information) should be kept only for as long as there is a legitimate business need. While the FTC applies a "reasonableness" standard without any definitive time period stated in the general rule, the agency views stale data as not particularly useful. The FTC therefore takes the position that such data should be purged to minimize the chance that it is compromised through a hack or other data breach incident. In addition to the FTC's general rule, certain types of data are subject to additional, more specific laws relating to data retention and storage.

4) If personal data is being stored, consider methods such as encryption and anonymization to protect that information should a data breach occur.

Data collection and storage practices are evolving rapidly within organizations as a result of improving data analytics. Note that personal data extends beyond names, addresses, social security numbers and emails to a broad array of identifying information that can reasonably be linked to an individual (e.g., geolocation information, device identifiers, photos, voice recordings, etc.). Companies should consider encryption, anonymization or other means to protect that information.

These recent attacks provide a reminder of the risk of data breaches for companies doing business online. But the need for preparedness is not limited to e-commerce or other Internet business as any company can become a target of a hacking attack seeking corporate secrets, intellectual property or other information. Before hackers strike, companies would do well to review their response plans, data retention policies and insurance program.

--By Russell P. Cohen and Stephanie Sharron, Orrick Herrington & Sutcliffe LLP

Russell Cohen is a partner in Orrick's San Francisco office. Stephanie Sharron is a partner in the firm's Silicon Valley, Calif., office. They are two of the leaders of the firm's privacy, data security and Internet safety group.

The opinions expressed are those of the authors and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.