OCTOBER 10-16, 2008

MASS HIGH TECH

THE JOURNAL OF NEW ENGLAND TECHNOLOGY

Cyber-thieves have you targeted: Is your company ready?

Though data breaches have become a regular feature of the daily news, recent events suggest we may have seen only part of a much more pervasive threat. On Aug. 5 the U.S. Department of Justice announced indictments against an alleged international ring of cyber criminals who purportedly hacked into the computer systems of at least nine prominent merchants using novel and increasingly sophisticated technology.

While some of these breaches were already public, others were essentially breaking news with the indictments, even though they had allegedly transpired some time ago. Meanwhile, cyber criminals continue to develop new tools and tactics to circumvent prevailing security measures.

GUEST COLUMN

Mark Szpak

Kevin Jones

Anne Johnson

With proper planning, companies can manage and perhaps limit data breach exposure.

Robust compliance efforts are essential to mitigating the risk of a data breach. Such efforts not only may help make it less likely a breach will occur in the first place, but also help to ensure that the company has a persuasive story to tell should a breach occur, causing litigants and regulators to scrutinize the company's conduct.

A strong compliance effort begins at the top with an experienced executive or management group tasked with spearheading information security and ensuring coordination among departments.

Identifying the location of data at risk, both internally and with third parties, is a vital first step. Today, this includes not only "stored" data, but also "streaming" data, which appears to have become the target du jour for cyber criminals.

The company also must assess its existing safeguards and intrusion detection measures. While documentation of information security policies and plans is important, it is equally critical to strive for effective implementation, and to regularly revisit those policies as technology and circumstances change.

Negotiating contractual provisions to help protect against or minimize the implications of a data breach can be another key component of the company's strategy. Most companies rely on various third parties such as banks, card companies, vendors or marketing companies to help them process and safeguard personal information.

To the extent a company has leverage in negotiating with these third parties, it should consider seeking contractual data security commitments and indemnification provisions from them, as well as containing its own data security commitments under those contracts.

If evidence of a breach arises, the company should be prepared to respond quickly and aggressively, which requires having a crisis management plan in place.

The plan is to have procedures to ensure that evidence of a breach goes promptly to a designated crisis management team, including in-house counsel. The plan also should establish a procedure for investigating and containing any breach that is discovered. Such investigations may depend on the company's retention of audit logs or other potential evidence and may also require the help of outside forensic experts.

Finally, the plan should anticipate mounting a public relations response. Not only may the company have applicable reporting and disclosure obligations, but breaches also have increasingly become leading news stories, attracting public attention that threatens to portray the victimized company in an unduly negative light.

Nearly every state has a statute requiring companies to notify consumers and/or regulators when personal information is breached. For companies with a multistate presence, these laws present a major compliance challenge because they are not always consistent and they often hinge on technicalities. For companies with a multinational presence, foreign laws and regulatory requirements may present further complication.

Thus, in addition to navigating the complex requirements of multiple governing statutes, companies should be prepared to weigh the pros and cons of varying notification strategies and the potential effects upon regulatory scrutiny, the risks of adverse publicity (then or later), and the possible civil litigation that data breaches can spawn.

MARK SZPAK is a partner and **KEVIN JONES** and **ANNE JOHNSON** are associates in Ropes & Gray LLP's litigation department and data security and intrusion group. They can be reached at mark.szpak@ropesgray.com, kevin.jones@ropesgray.com and anne.johnson@ropesgray.com.