NJBIZ®
ALL BUSINESS ◆ ALL NEW JERSEY
May 7, 2018

VENDOR VEXATION

Third-party providers can open door to hackers

Riker Danzig partners, from left, Maura Smith, Brian O'Donnell and Michael O'Mullan. - AARON HOUSTON

BY MARTIN DAKS

A South Jersey physicians network got in hot water and had to shell out a lot of money recently after sensitive medical information on more than 1,600 patients became available online.

The security lapse wiped off the password protection on a supposedly secure site. It wasn't the fault of Virtua Medical Group — a Georgia-based transcription vendor accidentally caused the mishap during a software update — but the network announced in April it would pay $417,816 and improve data security practices in a settlement with the New Jersey Division of Consumer Affairs.

Although it was a third-party vendor that caused this data breach, VMG was held accountable because it was their patient data and responsibility to protect it, state officials maintained.

Indeed, businesses may be liable for a data breach caused by a third-party provider, said Brian O'Donnell, a partner and co-chairman of law firm Riker Danzig.

"Each state has its own laws for a data breach, and there are also federal regulations if medical records are involved," O'Donnell noted.

Depending on what kind of data is exposed in a third-party breach, the originator, or hiring company, could be sued by regulators "and by customers who trusted you with their information," said Riker Danzig Partner Maura Smith.

"The business could potentially be sued for failing to adequately protect the information, or for failing to notify individuals and taking appropriate action, and for failing to follow its own policies," Smith said. "These kinds of concerns can keep [chief information officers] and CEOs up at night."

Riker Danzig is representing a U.S.-based multinational that used a third-party provider's software packing in its overseas operations.

Said O'Donnell: "The vendor was compromised with malware, which in turn was downloaded to hundreds of its own customers, turning thousands if not millions of computers and laptops into useless bricks. In addition to the time and expense of flushing out their own systems, all these companies may be exposed to claims from their customers."

Engaging in due diligence, including a security audit of a provider, may help.

"Many downstream providers will agree to a security audit that can range from a simple review of the provider's policies and procedures all the way to elaborate penetration tests," said Michael O'Mullan, a Riker Danzig partner. "Many of our own clients request these kinds of audits of our systems, since we handle their sensitive data, and we generally agree to these audits."

Businesses may be able to purchase a liability policy to cover themselves if a third-party provider is hacked and customer information accessed.

"But you have to be careful in selecting a policy, and match the coverage you need with your risk appetite," Smith stressed.

Said O'Donnell: "If a third-party requests access to your data, start by finding out why they need it and whether you can limit it. Have a dialogue and find out how they'll protect it, and consider writing in an indemnity agreement into your contract with them, obligating then to have adequate insurance to cover you if your company gets sued as a result of the third-party provider's mistake."

A company that engages in thorough due diligence may be able to use that as a defense if it's sued as a result of a third-party provider hack, said Eric Levine, vice president of Lindabury, McCormick, Estabrook & Cooper and co-chair of the law firm's cybersecurity and data privacy practice.

"It's important to deal with cybersecurity and other issues up front, especially when you're dealing with a new vendor," Levine said. "Consider the depth of access to your data that they need, too. If a firm is just providing you with paper products, they don't need deep access to your data, so a cybersecurity audit may not be very important.

"But if it's a payroll processor and employee benefits provider with access to your sensitive information like social security numbers, bank accounts or medical information, you want to make sure that some kind of cybersecurity audit and other concerns are addressed in your contract," he added.

Proper internal training and company-wide communications are also important.

"Earlier this year, a New Jersey-based client in the professional services industry advised us their email server had been hacked," Levine said.

No personal information appeared to be accessed, but the law firm alerted its employees.

"Later that day, our human resources director received what appeared to be a routine request for information from that client," Levine said. "Normally she would have gone ahead and processed it, but because of the notification of the hack and in-house employee training she had just completed, she immediately contacted me, since I'm a lead contact for our firm's Incident Response Team."

Levine contacted the client, who said their company had not issued the email request. "So we deleted it, distributed another company-wide warning and celebrated the fact that we had avoided this attack," he said.