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

5 Lessons Health Care Cos. Should Learn From Cyberattacks

Law360, New York (July 9, 2015, 11:29 AM ET) --

Richard DeNatale

The American health care industry is under attack by sophisticated hackers seeking access to electronic medical records. Since January, three health insurers have announced major data breaches involving millions of records, with the largest one at Anthem Inc., involving nearly 80 million records. There have been dozens of smaller breaches as well. According to statistics kept by the U.S. Department of Health and Human Services, in 2009 the health care sector experienced 18 data breaches involving 500 or more individuals. In the first three months of 2015, more than 50 such breaches were reported.

These incidents bear similarities to the cyberattacks on the retail sector in 2013 and 2014. As one retailer after another fell victim, important lessons emerged on the best ways of preparing for attacks and responding to ones that occur. While some retailers made errors that exacerbated their losses, others were able to minimize harm through careful planning and effective response. While some companies incurred significant financial losses, others were able to shift a large portion of the costs to their insurers.

As the health care sector braces for the current wave of attacks, it remains to be seen which companies will profit from these lessons. The stakes are particularly high. Health care records contain far more detailed information than what a retailer typically holds. They are also more permanent, in that you cannot cancel and replace your Social Security number and medical history as you can with a credit card. Stolen medical data can be used to create fake IDs, make fraudulent insurance claims or purchase prescription drugs for resale. These factors make a consumer's medical data worth 10 times more on the digital black market than a stolen credit card number.

Health care providers whose records are compromised will be subject to a host of legal requirements beyond those that apply to retailers. For example, the Health Insurance Portability and Accountability Act requires notification to affected individuals, to HHS and, in some circumstances, to media outlets. Companies may also face claims for compensatory and statutory damages under state laws governing the disclosure of confidential medical information, such as the California Confidentiality of Medical Information Act.

What lessons can the health care sector learn from recent data breaches?

Here we offer five key points drawn from our experience managing insurance strategy and recovery efforts in the wake of major cyberattacks.

1. This Is Only the Beginning

When retail giant Target Corp. reported a data breach in late 2013, some observers believed that the wave of attacks on the retail sector had crested and that heightened vigilance would prevent future incidents. But the attacks persisted for another year and claimed dozens more victims.

In the wake of the Anthem breach, it is likewise tempting to think the worst is over for the health care sector. Unfortunately, history suggests otherwise. Hackers have shown an ability to use successful techniques over and over again against successive targets, making adjustments in their malware to escape detection. Health care plans and providers continue to present rich targets and have multiple vulnerabilities. Although federal law encourages health care providers to encrypt patients' personal data, the requirement has been controversial and many providers have resisted. Providers also have multiple points of entry available to hackers (e.g., laptops used by medical professionals, hospital billing and medical records servers, call center software and medical devices connected to the provider's network) which can increase the chances of a successful attack.

All this means the health care sector faces the daunting prospect of a sustained series of attacks. But it also means it is not too late to begin to implement the best practices learned from prior breaches. Companies that act now to improve preparedness and enhance insurance coverage will reap substantial benefits in the event they fall victim to a breach.

2. The Importance of Preparedness

The view is sometimes heard in C-suite discussions that it is better to invest in advanced technology designed to prevent and detect breaches than in other mitigation measures, such as crisis planning and insurance. But recent history has taught us that even the most robust security measures cannot eliminate the risk of a breach. The risk to the health care sector may be even higher now, given reports that a foreign government may be behind the attacks on Anthem and other health plans. State sponsorship would give hackers access to the most sophisticated cybertools and additional resources in planning and carrying out their cyberattacks.

In light of this grim reality, every health care company should view itself as a potential victim. If they have not done so already, providers and health plans should ensure they have detailed and updated protocols for breach response and ample insurance coverage for the cyber risks they face.

3. Coordinating the Response Effort

Responding to a cyberattack requires a multidisciplinary approach involving several departments, including information technology, legal, accounting, human resources, communications and risk management. Close coordination among these groups is critical. Each must understand how its work fits into the overall mission. Also, company executives should recognize that different groups within the company may have competing business needs. The IT department's culture of open discussion and rapid problem-solving may conflict with the law department's need to preserve evidence and assert privilege. Efforts by the accounting department to track costs and document expenses may seem to other groups like an administrative burden.

Insurance policies come with their own specific requirements, which may not be understood outside the risk management group. Companies that wait too long to consult with the insurance team may run afoul of policy provisions requiring insurer consent before retaining counsel and forensic experts. As another example, some cyberpolicies cover breach notification and credit monitoring costs only where notice is required by law, so companies may jeopardize coverage by announcing in public statements that statutory notice requirements have not been triggered.

Such tensions can usually be resolved in a way that accommodates the needs of all concerned. Problems arise, however, when a key constituency is left out of the dialogue. Then decisions will be made without a full understanding of the consequences and important interests may be inadvertently harmed.

4. Buying the Right Insurance

The costs of a cyberattack can be substantial. They include forensic investigation expenses; remediation costs to cleanse malware and restore lost data; costs for notifying customers and providing identity theft services; legal fees to oversee breach response and defend against regulatory proceedings and litigation; and assessments by the payment card brands.

In most cases, the only way to recoup these costs is through insurance. But one of the lessons from the retail breaches is that insurance recovery will vary greatly depending on the type of insurance a company has. Retailers who did not purchase cyberinsurance have found it difficult to recover. To be sure, traditional property insurance policies often provide coverage for damage to data or network hardware. And some commercial general liability policies continue to cover consumer claims for common law or statutory privacy violations. But in recent years, the American insurance industry has been fighting claims for data breach losses under traditional insurance policies, forcing policyholders to retain coverage counsel and engage in a lengthy claims process to obtain recovery.

Companies with cyberinsurance have fared better. But cyberpolicies come with their own set of problems. They are expensive and extremely complicated. Standard industry forms have not yet emerged. There are significant differences in the scope of coverage provided by the various policy forms currently on the market. The best way to address these uncertainties is to have coverage counsel review existing insurance policies and make recommendations for enhancing coverage as needed.

5. Active Management of Insurance Claims

A major data breach can put a company in a state of crisis. It may find itself beset on multiple fronts by law enforcement, regulators, customers, employees and the media. An effective response requires vigorous and decisive action that takes control of events and shapes desired outcomes. During the wave of retail breaches, the companies that suffered most were ones that were slow to implement a communications strategy, lost control of the media or created confusion with contradictory public statements. At the same time, we saw other companies minimize the impact of serious breaches by acting quickly to identify the scope of the compromise, put remedial measures in place and communicate with key constituencies.

A proactive approach is equally important in pursuing insurance. We recommend that companies take certain key steps within 14 days after discovery of a breach: (1) immediately notify all insurers; (2) have coverage counsel review relevant policies to determine which costs are covered and which are not; (3) develop an insurance strategy that identifies the specific steps that must be taken to obtain recovery; and (4) integrate the insurance strategy into the overall breach response plan.

Then going forward, companies should actively communicate with their insurers to set expectations, obtain necessary consents and manage information requests. In the aftermath of a cyberattack, insurance is a critical asset needed to fund the recovery effort. Management of insurance claims deserves the same level of focus and energy as other aspects of breach response.

—By Richard DeNatale and Celia Jackson, Orrick Herrington & Sutcliffe LLP

Richard DeNatale is a partner and Celia Jackson is special counsel in Orrick Herrington & Sutcliffe's San Francisco office. DeNatale has taught insurance law at the University of California, Hastings College of the Law.