Responding to Data Breaches

by Lisa Stewart Albright

Data breach risk impacts every business sector in the United States, particularly those industries collecting consumer information and healthcare organizations. According to the 2016 Ponemon Institute study, the average per capita cost of a data breach to a company in the United States was $221, with an average total organization cost of $7.01 million.[1] The healthcare and financial services industries have the most costly data breaches, partly due to fines and an above-average rate of lost business.[2] This article explores several steps private companies and healthcare organizations should take immediately following a data breach event.

Attacks can take the form of traditional hackers who penetrate network perimeters and gain access to secure systems, or can occur due to employee negligence or intentional misconduct. A growing threat comes from what is referred to as a phishing attack. The Federal Bureau of Investigation (FBI) recently issued a warning regarding this style of attack.[3] In it, the FBI explains that "schemers go to great lengths to spoof company e-mail or use social engineering to assume the identity of the CEO, a company attorney, or trusted vendor. They research employees who manage money and use language specific to the company they are targeting, then they request a wire fraud transfer using dollar amounts that lend legitimacy."

Needless to say, lawmakers and industry leaders are working hard to prevent data breaches and impose consumer protections, yet, as of today, there are no comprehensive federal laws directed to the imposition of consumer notice requirements when consumer personal information is exposed (though there are several federal acts that are implicated, including the Federal Information Security Management Act; the Veterans Benefits, Health Care and Information Technology Act; the Privacy Act; the Gramm-Leach-Bliley Act; the

Health Insurance Portability and Accountability Act; the Federal Trade Commission Act; the Telecommunications Act; and the Fair and Accurate Credit Transaction Act, to name a few). The Federal Trade Commission (FTC) also regulates industries through enforcement actions brought against companies that are alleged to have violated Section 5 of the FTC Act, which prohibits companies from acting unfairly or deceptively. The majority of states have enacted their own legislation governing a company's required response when a consumer data breach occurs.

In 2005, the state of New Jersey enacted legislation concerning the security of personal information retained by businesses.[4] Pursuant to New Jersey law, a breach of security is defined to mean "unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or any other method or technology that renders the personal information unreadable or unusable."[5] Personal information is defined to include, generally speaking, a name combined with a Social Security number, driver's license number (or state identification number), or an account number or credit/debit card number in combination with any required codes that permit access to an individual's financial account.[6] Even dissociated data that would, if linked with other data, constitute personal information is included in the definition if it is disclosed with the means to link the dissociated data together.[7]

New Jersey imposes specific requirements on companies after a breach of security occurs. "Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person."[8] The disclosures should be made "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement."[9] Significantly, New Jersey law provides that disclosures of security breaches shall not be required if it can be established that misuse of the information is not reasonably possible.[10] Additionally, businesses must notify the Division of State Police in the Department of Law and Public Safety for investigation or handling in advance of any disclosure to the impacted party.[11]

Based on the costs associated with a data breach event, several safeguards can be employed to avoid the necessity of making a public disclosure. Since, by definition, a breach of security only occurs when the personal information released to or accessed by an unauthorized party has not been secured by encryption, counsel should advise their clients to encrypt data containing personal information whenever possible. For example, the risk of a successful phishing attack would be greatly diminished if a company policy required all PDF documents to be encrypted when sent by email. In turn, the recipient could contact the sender to request the encryption key over the phone. Additionally, counsel could advise clients holding electronic data to segment data in different servers. For example, one server could house a database of customer names. A separate server could link the database in the first server to a second database of Social Security numbers and other personal information housed on the second server. If a server containing the database of customer names was compromised, there may be no data breach absent the additional breach of the second server and the link between the two databases.

Counsel should also advise clients to ascertain the scope and impact of a data breach event immediately after it occurs. Counsel should retain third-party data breach technical specialists to verify that the data breach event has ended, ascertain what files were impacted, determine whether any additional hacker tools remain on the compromised system and then assist a client in the development of technical, physical and procedural safeguards to lower the likelihood of success for a subsequent data breach.

Additional legal considerations should be taken into account if a data breach impacts a health plan, healthcare clearinghouse or healthcare provider (*i.e.*, a covered entity) or a business associate of a covered entity. The Health Insurance Portability and Accountability Act of 1996, as amended, and its implementing regulations (collectively for purposes of this article, HIPAA) regulates the activities of covered entities and their business associates with regard to protected health information. In general, protected health information (PHI) is individually identifiable health information (information that relates to the past, present or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present or future payment for the provision of healthcare to the individual) that is transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium.[12]

A breach is defined in the so-called breach notification rule of HIPAA as the acquisition, access, use or disclosure of unsecured PHI in a manner that is not permitted by HIPAA that compromises the security or privacy of the PHI.[13] Similar to New Jersey's definition, a breach only occurs if the PHI is unsecured (*i.e.*, the PHI is not rendered unusable,

unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology that has been specified in guidance issued by the secretary of the Department of Health and Human Services).[14]

So, there is no breach if the PHI that is accessed is secured in accordance with HIPAA and if the key to the encryption or other security measure has not also been accessed. Additionally, there are various exceptions to the definition of breach (*e.g.*, breach does not include an unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of the covered entity if made in good faith and within the scope of the person's authority, and if it does not result in further use or disclosure in a manner not permitted by HIPAA).[15]

If a covered entity or business associate discovers that unsecured PHI may have been compromised, it should immediately consider whether one of the fairly limited number of exceptions to the definition of breach applies. It is important to note that if unsecured PHI has been released and none of the enumerated exceptions apply, a breach is *presumed* unless the covered entity or business entity can demonstrate there is a low probability the PHI has been compromised. This places the burden of proof on the affected covered entity or business associate, and requires an assessment of, at least: 1) the nature and extent of the PHI involved (Is it particularly sensitive? What types of identifiers were involved?); 2) the unauthorized person who used the PHI or to whom the PHI was disclosed (Was it to someone who is a healthcare provider and would not use or further disclose the information?); 3) whether the PHI was actually acquired or viewed (Did the person with access immediately delete the PHI without viewing it?), and 4) the extent to which the risk of the PHI has been mitigated.[16]

It should be noted that if there has been a ransomware attack, a breach is presumed if the PHI has been encrypted and is no longer available to the covered entity or business associate.[17] In such an event, the attacker gains access to the entity's system and encrypts its data, holding it hostage until payment is received. A ransomware attack has a strong potential to disrupt a healthcare provider's ability to provide health services; it inflicts significant financial losses, can damage sensitive data beyond repair and undoubtedly will result in reputational harm. The best offense is a good defense, and there are a number of protective measures that have been recommended in recently issued guidance.[18]

If a breach has occurred, a covered entity or business associate must determine how to respond. The response will generally take various forms, all of which should be completed, including: 1) mitigation; 2) notification; and 3) education/prevention. The method of mitigation necessarily depends upon the nature of the breach. If malware has been detected, an entity should immediately act to isolate or quarantine the affected data and then work to remove the malware. If a breach was caused by misdirected correspondence, a covered entity should immediately notify the recipient and direct that the correspondence be returned or destroyed. The recipient may be asked to certify to its destruction and evince understanding that the PHI should not be further disclosed.

The breach notification rule requires that a covered entity notify each individual whose PHI is reasonably believed to have been breached without unreasonable delay and within no more than 60 days following discovery of the breach. Covered entities should ensure their business associates notify them of any potential breaches within a sufficient period of time (frequently, within no more than five days of the business associate's discovery of the potential breach) so the covered entity can meet its own HIPAA obligations.

The rule lists the required elements of these notifications, including a brief description of what happened; a description of the types of PHI involved; any steps individuals should take to protect themselves from potential harm (*e.g.*, credit monitoring); a brief description of what the covered entity has done to investigate the breach, mitigate the harm and protect against further breaches; and contact procedures for individuals to ask questions.[19] Additionally, notification must be given to the secretary of Health and Human Services or the secretary's delegate.[20] If fewer than 500 individuals are affected, the covered entity may maintain a breach log and, no later than 60 days after the end of the calendar year, notify the secretary of all breaches that occurred.[21] If there are 500 or more affected individuals, the notification must be contemporaneous with notification to the media, which is also mandated by the rule in such instances.[22] Depending upon state law, the state police may be required to be notified. In the event of a ransomware attack, covered entities are urged to contact a local FBI or United States Secret Service field office immediately.[23]

A covered entity's response to a breach should include a consideration of (depending upon the circumstances surrounding the breach) whether employee disciplinary action or education is necessary under its policies and procedures and as a way to prevent future breaches. If the breach occurred because an employee accessed PHI out of curiosity, or posted PHI on social media, the covered entity may turn to its disciplinary policy, and may also require all employees take a refresher course on their HIPAA obligations. All staff should be trained on best practices

and what they may and may not do with regard to PHI, and the consequences of failing to follow policies and procedures should be applied uniformly to all employees.

An ounce of prevention is worth a pound of cure, and no matter how good the cure, a business may not avoid penalty if its security is breached. Nonetheless, in this digital day and age, businesses must be prepared to respond to a data breach, and should consider the appropriate steps proactively so that if a breach occurs it is prepared. Implementation of policies and procedures that detail the steps that should be taken in the event of a security breach are both necessary and, in many industries, required by law. ⚖

Lisa Stewart Albright *is a partner in the law firm of Archer & Greiner in its Princeton office. She is a member of the firm's healthcare group and frequently advises clients with regard to the security of protected health information.*

ENDNOTES

1. Ponemon Institute, 2016 Cost of Data Breach Study: Global Analysis, 2 (June 2016), http://www-03.ibm.com/security/data-breach/.
2. *Id.*
3. Federal Bureau of Investigation, FBI Warns of Dramatic Increase in Business E-Mail Scams (April 4, 2016), https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams.
4. N.J.S.A. § 56:8-161, *et seq.*
5. N.J.S.A. § 56:8-161.
6. *Id.*
7. *Id.*
8. N.J.S.A. § 56:8-163(a).
9. *Id.*
10. *Id.*
11. N.J.S.A. § 56:8-163(c)(1).
12. 45 CFR § 160.103.
13. 45 CFR §164.402.
14. 45 CFR §164.403.
15. *Id.*
16. *Id.*
17. Department of Health and Human Services, Ransomware Fact Sheet, http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.
18. *See, e.g.*, Letter from the Secretary of Health and Human Services to the Health Care Industry (June 20, 2016).
19. 45 CFR § 164.404.
20. *Id.*
21. *Id.*
22. *Id.*
23. U.S. Department of Homeland Security, U.S. Dept. of Justice & U.S. Dept. of Health and Human Svcs., Ransomware—What It Is and What to Do About It (June 2016), https://www.justice.gov/criminal-ccips/file/872766/download.