Anthem's two small details that led to one big breach

James J. Giszczak, Dominic A. Paluzzi, Miriam L. Rosen | Wednesday, February 18, 2015

Since we first advised on the **Anthem data breach**, additional information about the breach has come to light that provides some lessons for all businesses. Two significant issues with Anthem's security appear to have played a role in making the Anthem breach potentially the biggest disclosed breach in the healthcare industry to date. The consequences of that breach also mean that depending on your organization's contract obligations and self-insured status you may have legal notice obligations under HIPAA.

The data was not encrypted

First, the personal information of the 80 million customers and employees taken in the breach was exfiltrated from a large database that was *unencrypted*.

While businesses certainly have to balance between protecting information and having it easily accessible for use, encrypting information, especially private and valuable information, is a fairly inexpensive process that could have made the information taken far less valuable to the hackers and harder to access as a bulk transfer. Encrypting the data would essentially have scrambled it, making it unreadable, unusable, and worthless to the hackers.

The downside for companies in encrypting data is that the information becomes harder to share internally and externally. Another downside is that encryption slows down an authorized user's ability to access the data as readily as the user might want. Many companies find that these business costs outweigh the benefits of encryption or other types of controls, such as random passcodes.

Anthem is a textbook example of what can happen to companies who make the decision not to encrypt. Federal law does not require health insurers to encrypt data. Some states, including Massachusetts and Nevada, require encryption of all personal information stored on laptops or other portable devices, or transmitted wirelessly. Anthem claims it does not operate in any of those states.

Entry was made via an employee's password

Second, Anthem now believes the database was infiltrated through use of an employee password by a Chinese state-sponsored operation to steal personal information of specific groups of people. *Bloomberg* **reports**: "The attack appears to follow a pattern of thefts of medical data by foreigners seeking a pathway into the personal lives and computers of a select group – defense contractors, government workers and others." Once accessed, the hackers used malware to steal the data.

Password protection is a critical issue for businesses. It is likely that insufficient controls on the company's password protocols allowed employees to pick passwords that were not strong enough.

Do we have notice obligations under HIPAA?

Depending on your contractual obligations with Anthem and if your organization's health plan is self-insured, you may have legal notice obligations under HIPAA. If your organization's health plan is fully insured by Anthem, both your group health plan and Anthem are covered entities, subject to HIPAA. However, under an administrative exemption, your group health plan is not subject to most of the requirements of the HIPAA Privacy Rule if your group health plan does not create or receive PHI (other than summary health information and enrollment/disenrollment information). When this exemption applies, Anthem is obligated to provide the required HIPAA breach notifications to affected individuals and the United States Department of Health and Human Services Office for Civil Rights (HHS OCR). However, if your health plan is self-insured and your organization simply contracts with Anthem to administer claims for benefits, the organization's health plan is still a covered entity, but Anthem is only a business associate. Depending on how the health plan's business associate agreement with Anthem assigns the responsibilities for reporting breaches of HIPAA, your organization's health plan (not Anthem) may be required to provide the required HIPAA breach notifications to affected individuals and HHS OCR.

It is critical to review your business associate agreement with Anthem to determine if breach notice obligations have been delegated to Anthem. Also, don't forget about the state breach notification laws – those will also apply in this massive breach of PHI (and PII).

What businesses can do to avoid a data breach

Given these two security flaws – unencrypted data and access through an employee password – businesses are once again reminded of the steps they can take to avoid becoming the next Target, Home Depot, Sony, or Anthem.

- **Recognize that your business is not safe.** All businesses are vulnerable, regardless of industry, size, or location. As we have seen time and again with data breaches impacting the retail, financial, healthcare, entertainment, and other industries, a data breach crisis is not limited to those businesses with credit card or financial information. The risks extend to the disclosure of private emails, personal employee information, private salary information, medical information, trade secrets, confidential business information, employee files, and others. *In other words, no data is safe. No business is safe.*
- **Implement data security precautions.** Businesses can implement data security precautions that can go

far in helping to reduce the likelihood of a breach and, at a minimum, reduce exposure. Some of these precautions can include: requiring users to use complex passwords with numbers, letters, and symbols – never 1234 or even a word that could be found in a dictionary – and requiring that passwords be changed frequently; security applications; firewalls; dual authorization; two-step verification; data encryption; data storage security; antivirus and malware protection with continuous updates to security hardware and software; device security; and user training and education. While the security precautions a business chooses to employ will vary, every business simply must employ appropriate precautions.

- **Train employees.** Many breaches come from employee-targeted phishing emails. As **Verizon Data Breach Investigations Report** pointed out, most breaches fit into one of nine patterns, and "[t]he most prolific is the old faithful: spear phishing." Phishing emails are well-crafted, personally/professionally-relevant emails sent to targeted users with an organization that prompts the user to open an attachment or click a link within the message. Once the user/target clicks on the link, malware installs on the organization's computer system, a backdoor or command channel opens, and the hacker can then extract data, delete data, and basically do whatever the hacker wants. While education will not prevent all breaches, it can go a long way in raising awareness for these types of attacks.
- **Get insurance.** Most off-the-shelf business insurance policies do not cover damages arising from a data breach. Many insurance companies offer cyber or data breach coverage, but it is something that has to be elected. Businesses should examine their current insurance policies to determine if they are covered and at an appropriate level. If their insurance does not cover a data breach, *obtain data breach/cyber security coverage* that will cover the business through all stages of a breach, e.g., response and notification expenses, business interruption, computer forensic costs, credit monitoring costs, public relations costs, and defense and liability expenses, among others.
- **Limit employee access.** Businesses should treat protectable information as if it is on a need-to-know basis. Meaning, only those who need access to it should actually have access to it. Businesses should work closely with their IT departments to restrict employee access to protect information.
- **Audit.** All businesses should have a data breach risk audit performed to determine their level of risk and add greater protections where risks and gaps are identified.
- **If you do not need it, destroy it.** Businesses do not have to protect what they do not have. So, if a business does not have a legal obligation to keep data and it does not otherwise need it, get rid of it. In fact, 30 states require such destruction by law. It is important that businesses have a plan for data retention and destruction. It is also important that if the destruction includes any personally-identifiable information, the policy should conform to any applicable state law regarding data/document destruction that might apply.
- **Have a response plan.** To minimize exposure, the most important document to have is an incident response plan. An effective plan includes all key personnel, which can include executives, technology, human resources, public relations, and legal. It is important to note that these key people do not all have to be employees of the organization; many times a business will consult with outside technology professionals, public relations, and legal to build an effective response plan.

For those organizations which may be impacted by the Anthem breach, it is important that employees are reminded of the following:

- As with any data breach, it is always recommended that you remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

- Anthem has indicated that all notices regarding the incident will be in written form and sent through the U.S. mail. Anthem is warning all potentially impacted individuals regarding scam email campaigns designed to capture personal information through a phishing scheme. They are designed to appear as if they are from Anthem and the emails include a "click here" link for credit monitoring. These emails are NOT from Anthem. As a reminder,
  - DO NOT click on any links in email.
  - DO NOT reply to the email or reach out to the senders in any way.
  - DO NOT supply any information on the website that may open, if you have clicked on a link in an email.
  - DO NOT open any attachments that arrive with an email.
  - DO NOT respond to any phone calls asking for any of your personally identifiable information or health information.

With the possibility of a data breach looming for every company, businesses can minimize their risk by taking proactive steps to make their organizations and their data less vulnerable. This should take priority for all businesses in 2015. We will continue to provide regular updates on data security measures for your organization and lessons we can all learn from the inevitable breaches to come.

For more information, please contact one of the attorneys listed below.

James J. Giszczak

Dominic A. Paluzzi

Miriam L. Rosen