Security and Health Plan Paranoia: A Focus on the Third Party

Summary

How well do you sleep at night knowing that your company's security environment may not be as secure as it should be? Ransomware, data breaches and information theft are all serious considerations that have significant monetary and reputation costs for the affected companies.

In 2016 alone, 328 health care firms in the United States reported a data breach and 16.6 million Americans had their sensitive information compromised due to breaches[1]. Data breaches are especially costly in the health care industry where Protected Health Information (PHI) and Protected Personal Information (PPI) are extremely valuable. To determine the total cost of a data breach, you must calculate the costs of experts who investigate the cause and fix the problem, notification and free credit monitoring subscriptions for affected customers, customer support, including staffing a hotline and building a website, and any fines and fees imposed by governing bodies. A study by IBM and Ponemon Institute titled "2017 Cost of Data Breach Study: United States" cited that the average overall cost of a data breach in the United States is $7.35 million, with $225 being the average cost of each stolen record. These costs are even more significant in the health care industry where the average cost of each stolen record is $380. The study also found that many factors influence the cost of the data breach. For example, having an Incident Response Team can reduce the average cost per record by nearly $26, while having third-party involvement in the breach adds nearly $24 to the cost of each record[2].

These figures prove that companies must fully understand the risks and benefits of the methods used to evaluate their third-party vendors' security posture. This paper introduces topics all companies should consider when evaluating and accepting security postures of third-party service providers.

The Root of the Problem

In 2013, Target experienced a cyberattack that stole contact information from more than 60 million Target customers and more than 41 million payment card account numbers[3]. In May 2017, the federal government ruled that the company must pay $18.5 million to 47 states and the District of Columbia to resolve state investigations into the cyberattack. That is the largest settlement ever for a data breach and pushed the total cost well beyond the fees Target incurred to diagnose and correct the breach and notify its customers. Also, the investigation determined that the hackers gained access to Target's computer gateway by stealing credentials from the company's third-party air conditioning vendor. Once the hackers had access, they installed malware in the customer service database system and captured names, phone numbers, email addresses, payment card numbers, credit card verification codes and other sensitive data.

It was that easy. An inadequate security control at one of Target's third-party vendors cost the company millions of dollars and did an unmeasurable amount of harm to the retail giant's reputation. Unfortunately, this is not an isolated incident. According to Soha System's survey on third-party risk management, 63 percent of data breaches can be tracked directly or indirectly to the access by third-party vendors[4].

Not only do a majority of breaches occur from a third-party vendor, but the number of cybersecurity incidents involving third-parties is increasing. In a study published by BuckleySandler LLP, in April 2016 titled "Data Risk in the Third-Party Ecosystem," 73 percent of respondents reported that cybersecurity incidents involving third-parties are increasing and difficult to manage. They also stated that 37 percent of respondents did not believe their primary third-party vendors would notify them if it experienced a data breach involving sensitive and confidential information,

and 73 percent of respondents did not believe their third-party vendors' vendors would notify them in the event of a breach on their end[5]. The data for the study is based on research sponsored by BuckleySandler LLP and Treliant Risk Advisors LLC and a survey independently conducted by Ponemon Institute LLC.

That same study listed seven findings that revealed the risk to data in the third-party ecosystem:

- Companies cannot confirm if a third-party vendor has had a data breach
- Companies cannot determine if third-party vendors share their information with other partners
- Companies rarely conduct reviews of vendor management policies and programs
- Companies lack confidence in third-parties' data safeguards, security policies and procedures
- Accountability for the correct handling of a company's third-party risk management is decentralized
- Senior leadership and boards of directors are rarely involved in third-party risk management
- Companies rely on contractual agreements instead of audits and assessments to evaluate the security and privacy practices of third-parties

These findings help us understand the potential risks third-party vendors pose to our bottom line. In the event of a security breach, there is a good chance your third-party vendor is at fault, but your company is ultimately responsible for that breach. That leads us to the question, "How well do you know your third-party vendor and the risks they pose?" It is your company's responsibility to ensure you receive the most accurate and relevant information possible regarding third-party vendors' security postures.

Security Considerations for the Health Care Payer or Provider

As holders of private data, such as PHI and PPI, companies such as Companion Data Services (CDS) have a commitment to their customers, the nation and themselves to understand and evaluate risk within the environments for which they are responsible. Companies, like CDS, are dedicated to keeping their promises to their customers by meeting and exceeding laws and best practices seen as "gold standards" in the health care industry.

In the health care industry, companies must exceed the requirements of the following certifications:

- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Federal Information Security Management Act (FISMA)
- International Organization for Standardization (ISO) 9001:2008
- Federal Risk and Authorization Management Program (FedRAMP) Ready
- Uptime Institute Tier III
- Payment Card Industry (PCI) Compliance

These frameworks take great resources to maintain but are essential in achieving optimum security levels. Companies must understand that an incident at a third-party vendor can easily nullify the time and work it spent securing its information. That is why it is imperative to understand the security posture of your third-party vendors and service providers.

Below are questions companies should consider when deciding how to evaluate risk from third-party vendors:

Does security play a role in selecting and retaining third-party suppliers?

Given the risk posed by third-party vendors, companies must have adequate processes and policies in place to understand and consider the security posture of potential third-parties when selecting or retaining a vendor. At CDS, senior executives and board members receive periodic security updates that drive requirements and communicate the importance for having a developed and proven system for adequately assessing risk based on the work being performed by the third-party provider.

Which approach can be best utilized to have some comfort with your risk posture?

Your approach in assessing third-party risk should appropriately address the growing concerns in a complex and hostile cyber environment. Procedures must properly provide an objective assessment of your company's third-party vendors' security posture against those concerns.

Typically questionnaires or assessments are used to determine risk for third-party vendors. Both options have advantages and disadvantages, but each company must understand and evaluate its third-party vendors when deciding which security verification approach to use. For instance, should a vendor responsible for janitorial services be assessed similarly to a contractor who processes medical claims containing private health information? Probably not. The criteria for deciding the approach should be treated differently and distinctly, and each should be tailored to your company's mission.

What value does a questionnaire bring?

If your company suffers a security breach as a result of a third-party, a security questionnaire may not be much help. As in the Target breach, Target was responsible for paying $18.5 million in damages even though the breach resulted from a third-party vendor's weakness. The security questionnaire does not protect your company from monetary or reputational repercussions. The information gained to make an honest assessment as the basis for a decision to either partner with or require the vendor to remediate deficiencies is the only protection. It will only come if the questionnaire is relevant, accurate and properly scrutinized.

A questionnaire approach brings only as much value as the questions asked and the answers provided on the questionnaire by the third-party. For a questionnaire to be effective, the questions asked must be tailored to the individual vendor. A generic approach to questioning may not capture the true risk your company may be about to take in partnering with the third-party.

Below are some sample questions that CDS finds useful when understanding a vendor's security posture in the health care sector:

- Do you adhere to HIPAA guidelines to protect the privacy and security of health information?
- Do you adhere to HITECH requirements associated with the privacy and security concerns associated with the electronic transmission of health information?
- Do you have a recognized and applicable security framework to secure your systems?
- Do you adhere to federal, state and local laws?
- What are your PCI compliance requirements?
- What is your Tier III rating with the National Uptime Institute for Data Centers?

What value does an independent assessment bring?

An independent assessment conducted against a unified set of controls using a reputable and recognized assessor brings an immediate common understanding to the scope and objectivity of the assessment. Typically an assessment report provides the company with an objective and comprehensive review of the vendor's security and privacy practices against a widely accepted security control framework. Also, the signature from a reputable assessment firm verifies the validity and value of the report. Although the initial cost of an independent assessment may be more than a questionnaire, the actionable knowledge gained by an independent assessment makes the value well worth the initial investment.

CDS obtains multiple independent assessments each year from independent audit firms as a result of our numerous governmental and commercial customers. These audit firms systematically scrutinize every aspect of our security program both in documentation and execution. Upon completion, our customers (both governmental and commercial) receive a report which objectively identifies compliance or deficiencies in our security program with a recommendation to a solution.

How much can a third-party partner share?

In many industries, the companies you partner with today can, and will, become competitors in the future. Knowing this, it is understandable that third-party vendors are not willing to share how they execute the security requirements imposed by contractual agreements or governmental regulations. Assessments are more likely to be accurate when a vendor is not concerned about a competitor receiving proprietary information about how it handles security due to non-disclosure agreements with the independent assessor. Every independent assessment performed on CDS includes a non-disclosure agreement between the audit firm and CDS, alleviating proprietary information concerns and adding to the accuracy of the assessment.

Conclusion

Evaluating the risk posture of third-party vendors is imperative. It is up to you to decide if your company should evaluate by attestation or by independent assessment? How you do it is less important than having fully supported programs that are tailored to the information you process. This results in accurate, objective and timely information about the state of your third-party vendors' security and privacy programs.

By partnering with CDS, you gain the assurance that allows you to sleep well at night, knowing that you understand the complete risk in your security environment and the repercussions of risk becoming a reality.

CDS and our parent company support combinations of Medicare, Medicaid, TRICARE, Federal Employee Health Benefits Program and Medicare Advantage health plans, as well as commercial health plan business and infrastructure systems. More than 6 percent of all health care expenditures in the United States are processed through health care systems that CDS developed, maintains or is operationally executing.

Safeguarding data is our major concern. Safety measures extend to human capital, facility and data access, preservation and telecommunication data transmissions. These measures are reinforced with annual training programs that focus on industry-accepted and mandated standards for accessing, handling and safeguarding data. Data center security encompasses a broad set of policies, technologies and controls designed to protect data, applications, infrastructure and its physical location. Our multilayered approach to security provides peace of mind through:

- Administrative safeguards that prevent, detect, contain and correct violations
- Physical safeguards including, facility access, workstation use, device and media controls designed to prevent and contain incidents
- Technical safeguard, including access, audit, authentication and transmission security

In the ever-changing health care universe, ensuring an economical, dependable and secure hosting environment is our priority.

[1] "Healthcare Breach Report 2017" Bitglass, May 3, 2017. https://www.bitglass.com/press-releases/2016-healthcare-breaches-all-time-high. Accessed Sept. 21, 2017.

[2] "2017 Cost of Data Breach Study: United States" Ponemon Institute, June 2017. https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03130wwen/SEL03130WWEN.PDF. Accessed Sept. 25, 2017.

[3] "Target to pay $18.5M for 2013 data breach that affected 41 million customers" USA TODAY, May 23, 2017. https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/. Accessed Aug. 17, 2017.

[4] "Third Party Access is a Major Source of Data Breaches, yet Not an IT Priority" Soha Systems, 2016. http://go.soha.io/hubfs/Survey_Reports/Soha_Systems_Third_Party_Advisory_Group_2016_IT_Survey_Report.pdf?t=1467123126371. Accessed Aug. 17, 2017.

[5] "Data Risk in the Third-Party Ecosystem" Ponemon Institute, April 2016. https://www.ponemon.org/local/upload/file/Data%20Risk%20in%20the%20Third%20Party%20Ecosystem_BuckleySandler%20LLP%20and%20Treliant%20Risk%20Advisors%20LLC%20Ponemon%20Research%202016%20-%20FINAL2.pdf. Accessed Aug. 17, 2017.