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.

From 2019-2020, the number of healthcare breaches rose by:

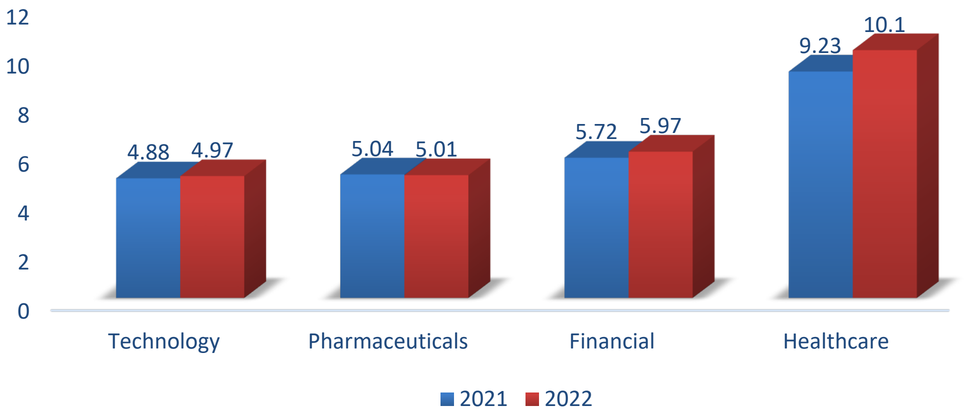
55%

In 2020 there were 599 health care breaches reported in the United States, a 55.1 percent increase from 2019. More than 24 million individual records were disclosed by these breaches with an estimated cost of more than $499 per record[1]. Traditionally, data breaches are especially costly in the health care industry due to the high value of Protected Health Information (PHI) and Protected Personal Information (PPI).

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 fines and fees imposed by governing bodies.

A recent study by IBM and Ponemon Institute cited that the average overall cost of a data breach in the U.S. in 2022 was estimated at $4.35 million dollars. However, the study noted that costs are substantially higher in the health care industry, reaching a record high of $10.10 million per breach this year. The study found that many factors influence the cost of the data breach. For example, employing a zero-trust architecture reduces per breach cost by roughly $1million or that hybrid cloud approaches tended to reduce breach cost by 27.6 percent over pure cloud solutions[2].

Average Cost of a Data Breach By Industry (in millions)[2]



These figures prove that companies must fully understand the risks and benefits of the methods used to evaluate their security posture. This paper introduces topics all companies should consider when evaluating and accepting security architectures, solutions and integration partners.

The Root of the Problem

Business system solutions continue to be rapidly integrated into public Cloud Service Provider (PCSP) environments. The ability to leverage public cloud commoditized network, storage and compute resources on demand and consume prebuilt infrastructure and application services are desirable for many businesses application functions. Public cloud however provides only partial control coverage for its respective system security frameworks. This is a natural outcome as the cloud provider cannot extend their control practices into the customer space. The adoption of public cloud driven infrastructure and services often result in an assumption that hosted business systems derive their security posture solely from the cloud provider. This is not the case. While the cloud providers can supply best practices, the security posture of the business system must extend back to the business owner. More than 45 percent of all data breaches were cloud based in 2022 and the average cost of each breach was 27.6 percent higher than breaches from hybrid implementations.

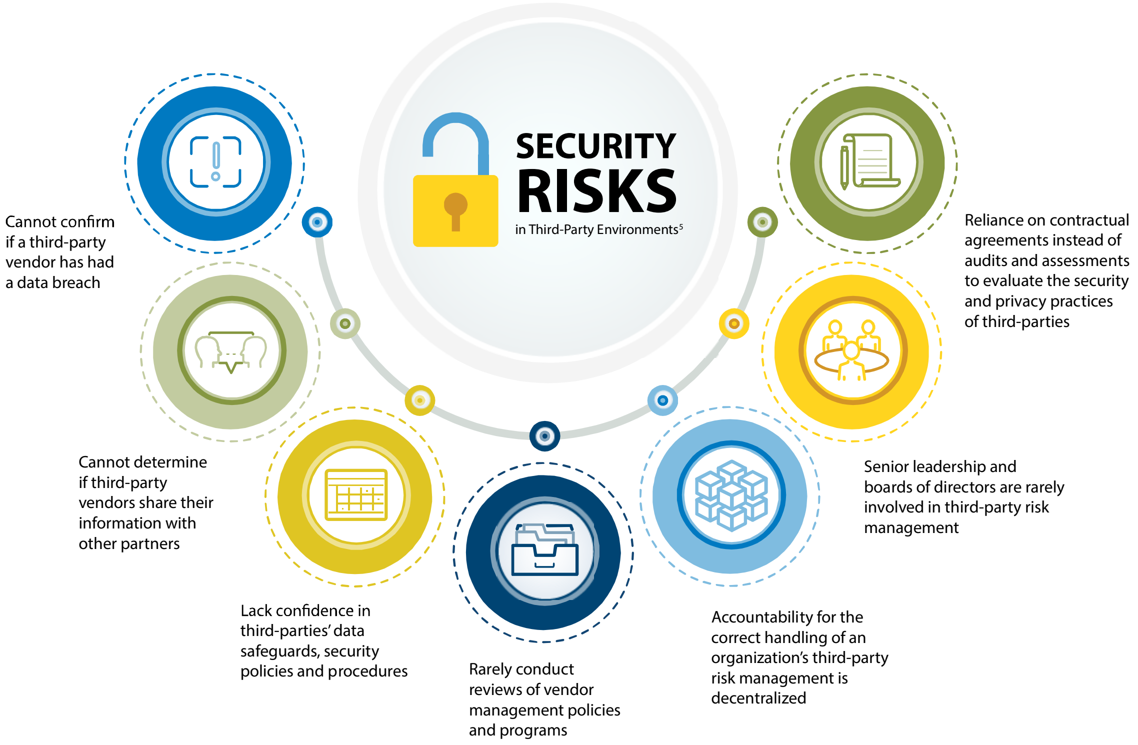
Therefore, the successful adoption of cloud services requires effective third-party vendor risk management to include the public cloud components of an enterprise application portfolio. Deficient third-party vendor risk management continues to expose health care organizations.

In 2022 the majority of the largest health care breaches stemmed directly from security issues involving third party vendors, many of them cloud based[4].

Not only do most breaches occur as a result of third-party vendors, but the number of cybersecurity incidents involving third parties is increasing, and third-party data breaches are prevalent. In a recent study, 59 percent of respondents experienced a cybersecurity incident caused by a third party. Also cited was that 34 percent of respondents did not believe their primary third-party vendors would notify them if they experienced a data breach involving sensitive and confidential information[5].

There are seven key contributors to high data breach risk 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.


SECURITY
RISKS
in Third-Party Environments[5]
Cannot confirm if a third-party vendor has had a data breach
Cannot determine if third-party vendors share their information with other partners
Lack confidence in third-parties' data safeguards, security policies and procedures
Rarely conduct reviews of vendor management policies and programs
Accountability for the correct handling of an organization's third-party risk management is decentralized
Senior leadership and boards of directors are rarely involved in third-party risk management
Reliance 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. This reality leads 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, LLC (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 meeting and exceeding laws and best practices seen as "gold standards" in the health care industry.

In the health care industry, companies must exceed these certification requirement frameworks:

- 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) 9001:2015
- International Organization for Standardization (ISO) 27001:2013
- Uptime Institute Tier IV

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 employ adequate processes and policies 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 of having a developed and proven system for adequately assessing risk based on the work being performed by the third-party provider.

Companion Data Services, LLC and its respective marks are trademarks of Companion Data Services, LLC. Because we are continuously improving our solution offerings, Companion Data Services reserves the right to change specifications without prior notice and disclaims all liability for any inaccuracies in this document including, without limitation, those arising from changes in solution offerings or from changes in technology. This material is a confidential, proprietary or trade secret product of Companion Data Services. Any unauthorized use, reproduction or transfer of these materials is strictly prohibited. For more information visit: companiondataservices.com.

Which approach can be best used 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 PHI? Probably not. The criteria for deciding the approach should be treated differently and distinctly and 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. 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. An insightful and unbiassed assessment will only be realized 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 uses to understand 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 well established architectural principles such as least privilege and zero trust that can mitigate social engineering attack vectors?
    - What mitigations are in place with regards to Phishing and other email attacks?

- Do you adhere to federal, state and local laws?
- How are you assessed?
- How do you continuously monitor and report your systems security risk?

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 report’s value. 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 worth the initial investment.

CDS obtains multiple independent assessments each year from audit firms, resulting from 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 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 can and will become your future competitors. Therefore, 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 assessment’s accuracy.

> **TRUST but**
> **VERIFY**
>
> - Ronald Reagan

Conclusion

Evaluating the risk posture of third-party vendors is imperative. You must decide if your company should evaluate by attestation or by independent assessment? How you do this 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 U.S. 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 2021" Bitglass, Feb 3, 2021. 2021 Healthcare Breach Report (bitglass.com). Accessed Nov. 22, 2022.

[2] "Cost of Data Breach 2022" IBM, July 7, 2022. Cost of a data breach 2022 | IBM. Accessed Nov. 22, 2017.

[3] "Breaches exposed 45.67M patient records in 2021, largest annual total since 2015" SCMedia, Jan 31, 2022. Breaches exposed 45.67M patient records in 2021, largest annual total since 2015 | SC Media (scmagazine.com). Accessed Nov. 22, 2022.

[4] "Biggest Healthcare Data Breaches Reported This Year, So Far" Sept 2, 2022. Biggest Healthcare Data Breaches Reported This Year, So Far (healthitsecurity.com). Accessed Nov. 22, 2017.

[5] "The 2022 Data Risk in the Third-Party Ecosystem Study" Sept 6, 2022, Ponemon Institute (Sponsored by RiskRecon). Accessed Nov. 22, 2022.