Health3PT

The State of Healthcare Third-Party Cyber Risk Management

Findings from an independent survey of Covered Entities and Business Associates in the U.S. Healthcare industry, conducted April-June 2023.

Purpose:
The Health3PT Initiative conducted the survey summarized on the following pages to identify issues in the current Healthcare Third-Party Cyber Risk Management environment and drive towards improved collaborative solutions.

You're invited to review aggregated respondent results to gain valuable insights from other healthcare information security professionals that can help your organization create a healthier, lower-risk ecosystem for all participants.

The State of Healthcare Third-Party Cyber Risk Management 2023
Health3PT Survey Results

Why Effective Third-Party Risk Management Is So Important

Vendor risk is a serious problem in healthcare today because:

55%	of healthcare organizations experienced a third-party breach in the past year[1]
$10.1M	is the average cost of a healthcare data breach[2]
90%	of the most significant healthcare breaches in 2022 were tied to vendors[3]

[1] https://www.hipaajournal.com/55-of-healthcare-organizations-suffered-a-third-party-data-breach-in-the-past-year/
[2] https://www.ibm.com/reports/data-breach
[3] https://www.scmagazine.com/feature/breach/most-of-the-10-largest-healthcare-data-breaches-in-2022-are-tied-to-vendors

Introduction

Third-party risks associated with supply chain vendors and service providers critically threaten and challenge healthcare cybersecurity, data protection, and the safety of patient records. Unfortunately, today's methods to manage third-party risk exposure are burdensome and inadequate.

There are significant blind spots relating to third-party information security risk because:

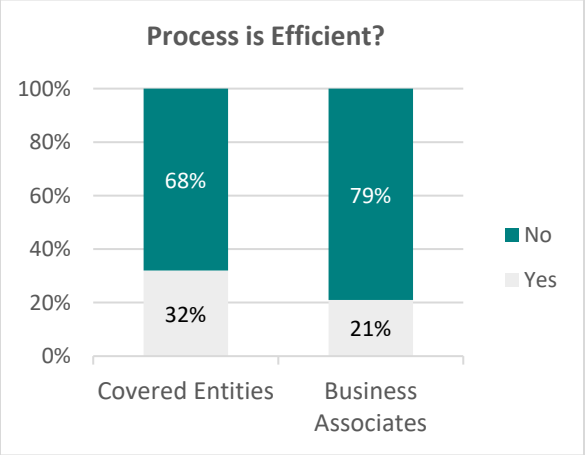
- Each organization and each vendor handle their assessments differently and often manually.
- Relying parties often lack the resources to follow up on vendor risk remediation efforts.
- Most assurances do not consistently show that proper information security controls are in place.

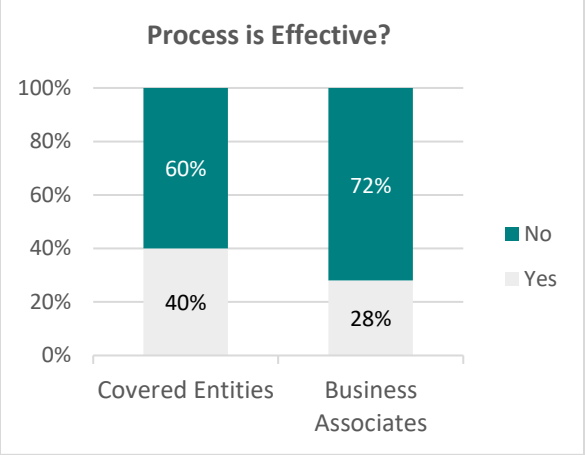
To establish and promote trusted cybersecurity practices throughout the third-party healthcare ecosystem, professionals from leading healthcare organizations joined to form the Health 3rd Party Trust (Health3PT) Initiative. The objectives of the Health3PT-sponsored survey were to identify common issues around healthcare TPRM and gather respondent insights on collaborative ways to refine and implement meaningful and improved solutions.

Summary of Key Findings

1. Covered Entities and Business Associates

Both groups share a strong belief that current TRPM processes are inefficient and ineffective in preventing data breaches:





2. Suggested Improvements from Both Sides
Survey results point to several efficiencies that can create a more collaborative approach that helps streamline and standardize the risk management process for Covered Entities and Business Associates.

- Create norms around inherent risk and vendor tiering in the TPRM ecosystem.
- Increase trust by standardizing around third-party validated assurance mechanisms instead of one-off self-attested questionnaires to improve efficiency and effectiveness on both sides.
- Share assessment results electronically to improve efficiency and effectiveness while delivering faster time to insights.
- Driving constant security improvement through continuous monitoring and remediation reporting.

About the Survey

The survey is designed to capture perspectives from healthcare Covered Entities and Business Associates.

Covered Entities. Under HIPAA rules, Covered Entities are defined as (1) health plans, (2) healthcare clearinghouses, and (3) healthcare providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards. Covered Entities must require Business Associates with whom they partner to meet applicable HIPAA requirements.

Business Associates. Under HIPAA rules, Business Associates are defined as a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

187
Total Respondents
59
Covered Entities
128
Business Associates
April-June 2023
Survey Conducted

The survey responses not only help validate why and where third-party risk management methodologies can be improved, but also reveal where opportunities exist that can build more efficient and practical approaches to reduce cyber risk across the healthcare ecosystem.

Executive Summary

Survey questions were designed to gain an understanding of the standard practices used by healthcare organizations to assess the cyber risk of their suppliers and how those suppliers provide assurances of their cybersecurity capabilities. The complete data set in the Appendix will provide insights into how current practices reveal gaps in assessment quality, frequency, and continuous monitoring of remediation efforts that are central to more effective risk management. This section focuses on the top-level findings around the most significant challenges and where organizations need help to make TPRM more effective.

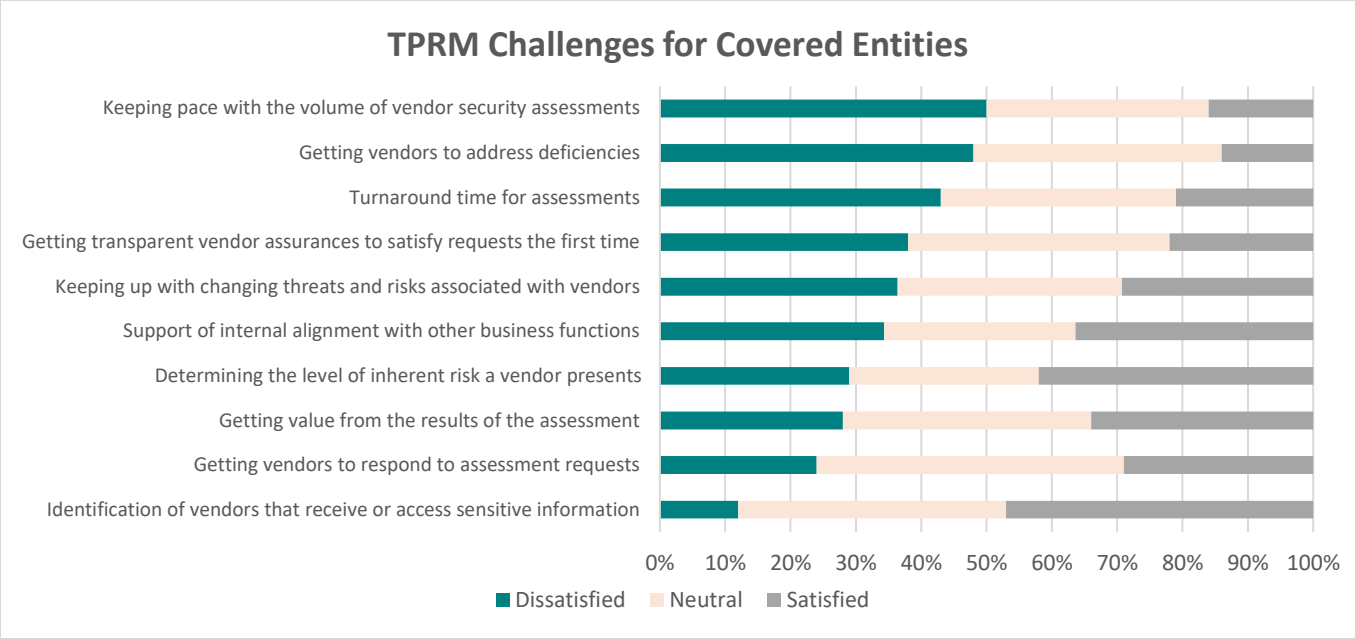
Primary Challenges and Pain Points

The Health3PT survey gathered information from Covered Entities and Business Associates to identify pain points in the current process and pinpoint opportunities for improvement. In addition, each group

was asked how satisfied they were that their organization could address the common challenges associated with the current TPRM processes.

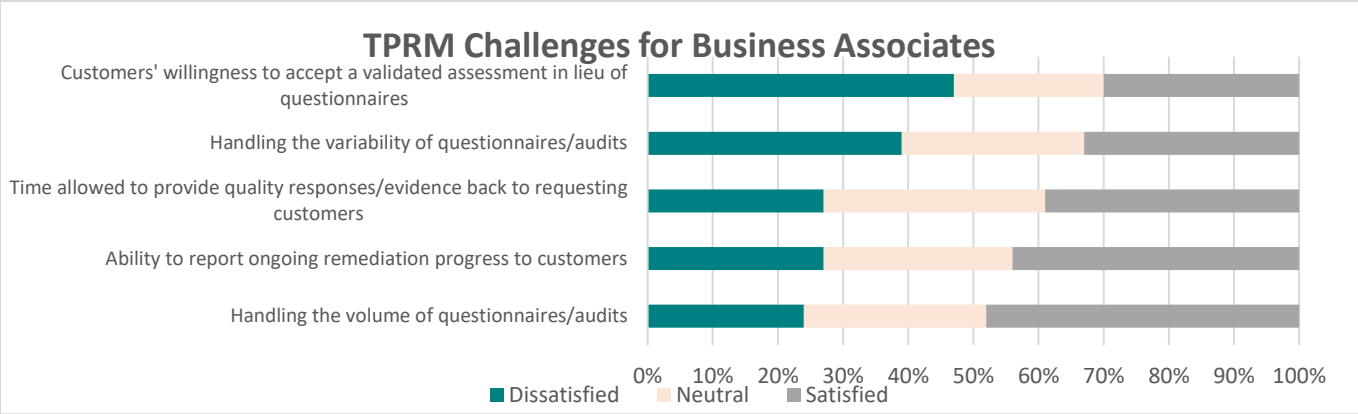
Covered Entities: From the table below, you can see that most organizations need help with these aspects of TPRM:

- Keeping pace with the volume of security assessments they receive.
- Getting vendors to address and fix identified information security deficiencies.
- Excessive turnaround time for assessments.
- Receiving transparent assurances from vendors to satisfy the request the first time.



Business Associates: From the table shown below, you can see that most organizations need help with these aspects of TPRM:

- Customers unwilling to accept third-party validated assessments and certifications in place of proprietary control questionnaires.
- Handling the variability of questionnaires and audits.
- The resources and time required to meet compliance requirements.



The State of Healthcare Third-Party Cyber Risk Management 2023
Health3PT Survey Results

Key Survey Takeaways

The State of Healthcare Third-Party Cyber Risk Management survey confirms and highlights several significant findings:

- Both Covered Entities and Business Associates feel overwhelmed and report substantial challenges with current healthcare TPRM processes.
- Business Associates experience audit fatigue from the sheer volume and variability of proprietary security questionnaires they receive from their customers.
- Covered Entities can't keep pace with the volume of questionnaire responses they receive from their vendors, and they often need to follow up because information they receive rarely satisfies the request the first time.
- Neither party sees the current process as effective to prevent data breaches.
- There is a shared vision for a desired future state that adds efficiency by leveraging additional collaboration, standardization, and automation.

Health3PT Recommended Practices for Better TPRM

By combining survey learnings with perspectives shared at a recent Vendor Risk Management Summit and long-standing experience from healthcare information security and risk management professionals, Health3PT recommends the following Best Practices for TPRM success:

1. Concise contract language tying financial terms to a vendor's transparency, assurance, and collaboration on information security matters.
2. Risk tiering strategies that drive the frequency of reviews, the extent of due diligence, and the urgency of remediation.
3. Appropriate, reliable, and consistent assurances of security capabilities based on the vendor's level of inherent risk.
4. Follow-up through to close identified gaps – including formal Corrective Action Plans (CAPs).
5. Recurring updates of vendor assurances.
6. Metrics and reporting on organization-wide vendor risks.

Establishing and adopting these more effective and efficient TPRM processes will transition TPRM in healthcare from a superficial check-the-box exercise that exposes organizations to unnecessary risks to more robust, collaborative information protection programs that ultimately will benefit all participants across the healthcare community.

The guiding principles for the Health3PT Initiative are…

- Collaboration and standardization move us forward.
- Incremental progress is important.
- True partnerships with vendors are key.
- Some compromise will be necessary to make progress.

About Health3PT

The Health 3rd Party Trust Initiative is governed by a council of professionals from leading care providers, health systems, and other healthcare organizations committed to reducing third-party information security risk with more reliable and consistent assurances. **health3pt.org**

Appendix

This Appendix shows each survey's exact questions and answers for Covered Entities and Business Associates.

Covered Entities (n=59)

Challenges

1. How satisfied are you that your organization can effectively address these common risk management challenges?

Challenge	Dissatisfied	Neutral	Satisfied
Identification of vendors that receive or access sensitive information	**12%**	**41%**	**47%**
Determining the level of inherent risk a vendor presents?	**29%**	**29%**	**42%**
Getting vendors to respond to assessment requests?	**24%**	**47%**	**29%**
Receiving transparent assurances from vendors to satisfy the request the first time	**38%**	**40%**	**22%**
Keeping pace with the volume of vendor security assessments	**50%**	**34%**	**16%**
Turnaround time for assessments	**43%**	**36%**	**21%**
Getting value from the results of the assessment	**28%**	**38%**	**34%**
Getting vendors to address deficiencies	**48%**	**38%**	**14%**
Support of internal alignment with other business functions	**34%**	**29%**	**36%**
Keeping up with changing threats and risks associated with vendors	**36%**	**34%**	**29%**

Current Practices

2. Do you have contractual language for security requirements that must be met before onboarding a vendor?
    a. **85%** Yes
    b. **15%** No
3. What forms of assessments do you accept from your vendors today? (Choose all that apply)
    a. **14%** SIG Questionnaires
    b. **27%** Custom/Proprietary Questionnaires
    c. **27%** Third-party Validated Assessment Opinion Reports (SOC 2)
    d. **27%** Third-party Certification Reports (HITRUST, ISO)
    e. **5%** Other
4. If you use surveys or questionnaires to assess third-party risk, what framework(s) or standards are they based on? (Choose all that apply)
    a. **23%** NIST (800-53, 800-171)
    b. **8%** SIG
    c. **20%** NIST CSF
    d. **15%** ISO 27001-2
    e. **23%** HITRUST
    f. **8%** AICPA Trust Services Criteria
    g. **3%** None of the above

5. What percentage of your vendor population does your organization assess?
    a. **9%** <5%
    b. **3%** 6-10%
    c. **24%** 11-25%
    d. **17%** 26-50%
    e. **27%** 51-80%
    f. **20%** >81%
6. What percentage of your vendor population is regularly reassessed (at least annually)?
    a. **29%** <5%
    b. **9%** 6-10%
    c. **27%** 11-25%
    d. **15%** 26-50%
    e. **8%** 51-80%
    f. **12%** >81%
7. How do you obtain updates on remediations from your vendors?
    a. **12%** Vendors proactively update us as they remediate gaps.
    b. **29%** We reach out for a status update on all remediation actions.
    c. **36%** We reach out for status updates based on gaps or vendor criticality.
    d. **8%** We revisit remediation updates at the time of contract renewal.
    e. **15%** We do not receive remediation updates.
8. Do you believe your current vendor risk management process is efficient (value vs. effort)?
    a. **32%** Yes
    b. **68%** No
9. Do you believe your current vendor risk management process is effective in terms of preventing data breaches?
    a. **40%** Yes
    b. **60%** No

Indicators to establish a better TPRM model:

10. Please indicate the level of importance for each statement below in terms of making vendor risk management more efficient and effective.

Statement	Unimportant	Neutral	Important
Create norms around inherent risk and vendor tiering in the TPRM ecosystem	**3%**	**12%**	**85%**
Standardize around third-party validated assurance mechanisms instead of one-off self-attested questionnaires to improve efficiency and effectiveness on both sides	**5%**	**10%**	**85%**
Receive vendor assessment results electronically to gain faster time to insights and enable your resources to do higher value risk management activities	**9%**	**7%**	**84%**
Drive constant security improvement through continuous monitoring and remediation reporting	**2%**	**14%**	**84%**

The State of Healthcare Third-Party Cyber Risk Management 2023
Health3PT Survey Results

Covered Entity Respondents Firmographics

11. What is your role in the organization?
    - **10%** C-level
    - **31%** VP/Director
    - **36%** Manager
    - **23%** Other
12. In which department do you work?
    - **56%** IT Security
    - **10%** Vendor Risk Management
    - **2%** Procurement
    - **25%** Compliance
    - **7%** Business/Other
13. What is the size of your organization in annual revenue?
    - **27%** <$100M
    - **20%** $101-$499M
    - **11%** $500-$999M
    - **25%** $1B-$5B
    - **17%** >$5B

Business Associates/Vendors/Suppliers (n=128)

Challenges

1. How satisfied are you that your organization can effectively address these common risk management challenges?

Challenge	Dissatisfied	Neutral	Satisfied
Handling the volume of questionnaires/audits	**24%**	**28%**	**48%**
Handling the variability of questionnaires/audits	**39%**	**28%**	**33%**
Time allowed to provide quality responses/evidence back to requesting customers	**27%**	**34%**	**39%**
Ability to report ongoing remediation progress to customers	**27%**	**29%**	**44%**
The willingness of customers to accept validated assessments and certifications in lieu of their proprietary control questionnaires	**47%**	**23%**	**30%**

Current Practices

2. What percentage of your customers ask for cybersecurity assurances to enable a business relationship?
    a. **5%** <5%
    b. **4%** 6-10%
    c. **11%** 11-25%
    d. **10%** 26-50%
    e. **20%** 51-80%
    f. **50%** >81%

3. What percentage of your customers regularly reassess your organization or ask to see progress on remediation?
    a. **10%** <5%
    b. **11%** 6-10%
    c. **20%** 11-25%
    d. **13%** 26-50%
    e. **24%** 51-80%
    f. **22%** >81%
4. What assurance mechanisms do you provide to fulfill customer cybersecurity requests (Check all that apply)
    a. **14%** SIG Questionnaires
    b. **28%** Custom/Proprietary Questionnaires
    c. **22%** Third-party Validated Assessment Opinion Reports (SOC 2)
    d. **28%** Third-party Certification Reports (HITRUST, ISO)
    e. **6%** Other
5. If you selected C or D in question 4, what percentage of your customers will forgo the use of their proprietary questionnaire during security due diligence if you provide a third-party validated assessment or certification?
    a. **23%** <5%
    b. **10%** 6-10%
    c. **15%** 11-25%
    d. **19%** 26-50%
    e. **15%** 51-80%
    f. **7%** >81%
    g. **11%** Not applicable
6. Do you believe the current process for providing cyber risk assurances is efficient?
    a. **21%** Yes
    b. **79%** No
7. Do you believe the current process of providing cyber risk assurances effectively prevents data breaches?
    a. **28%** Yes
    b. **72%** No

Indicators to establish a better TPRM model:

8. Please indicate the level of importance for each of the potential solution elements below.

Statement	Unimportant	Neutral	Important
A collaborative approach to understanding the assurance requirements of your organization based on the inherent risk you present to your customer.	**7%**	**12%**	**81%**
Standardize third-party validated assurance mechanisms that cover the scope of the business relationship instead of one-off questionnaires to improve efficiency and effectiveness on both sides.	**5%**	**8%**	**87%**
Ability to share your assessment results electronically to provide your customer faster time to insights and decision making.	**8%**	**11%**	**81%**

The State of Healthcare Third-Party Cyber Risk Management 2023
Health3PT Survey Results

Business Associate Respondents Firmographics

9. What is your role in the organization?
    - **30%** C-level
    - **38%** VP/Director
    - **15%** Manager
    - **17%** Other
10. What is the size of your organization in annual revenue?
    - **65%** <$100M
    - **16%** $101-$499M
    - **9%** $500-$999M
    - **5%** $1B-$5B
    - **5%** >$5B
11. What is your business category?
    - **6%** Healthcare Insurance
    - **8%** Hospital/Clinical Health Services Provider
    - **3%** Pharma/Biotech
    - **4%** Medical Device Manufacturer
    - **56%** Business Services (software, consulting, hardware)
    - **21%** Other