Third-Party Vendor Risk Management

cloud security alliance®

The permanent and official location for Health Information Management (HIM) Working Group is https://cloudsecurityalliance.org/research/working-groups/health-information-management/

© 2022 Cloud Security Alliance – All Rights Reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance at https://cloudsecurityalliance.org subject to the following: (a) the draft may be used solely for your personal, informational, non-commercial use; (b) the draft may not be modified or altered in any way; (c) the draft may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the draft as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance.

Acknowledgments

Lead Author

Dr. James Angle

Contributors

Michael Roza

CSA Global Staff

Vince Campitelli
Alex Kaluza
Claire Lehnert

The Health Information Management (HIM) Working Group aims to provide direct influence on how health information service providers deliver secure cloud solutions (services, transport, applications, and storage) to their clients, and foster cloud awareness within all aspects of healthcare and related industries.

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Table of Contents

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Abstract

Healthcare Delivery Organizations (HDOs) entrust the protection of their sensitive data, their reputation, their finances, and their business availability with third parties. A breach of their third-party vendors could mean a breach of their enterprise, so HDOs need to know: Are third-party vendors trustworthy? If so, why? If not, why not? Additionally, if not, what should be done about it? These questions are HDOs to answer and act on.[1] HDOs rely on third-party vendors to supply critical services. These services are often used to process or store Protected Health Information (PHI). Given the importance of third-party vendors, it is critical to identify, assess, and mitigate third-party cyber risks to ensure business resilience. The use of third-party vendors results in an expanded attack surface as attackers can breach the vendor and either extract data from the vendor or use the vendor to gain access to the HDOs systems. Cyberattacks target HDOs and their vendors in this expanded attack surface. It is incumbent on HDOs to ensure that their third-party vendors comply with data management policies and ensure the safety and security of the data entrusted to them.

Introduction

Healthcare organizations are struggling to identify, protect, detect, respond, and recover from third-party or vendor-related data breaches, vulnerabilities and threat events. However, current approaches to assessing and managing vendor risks are failing. The failure of current approaches to third-party risk management creates a real economic impact. Organizations encounter increasing Health and Human Services (HHS) and Office For Civil Rights (OCR) fines and investigations. There are several reasons why third-party risk management programs fail in healthcare:

> - The lack of automation and reliance upon manual risk management processes makes it difficult to keep pace with cyber threats and the proliferation of digital applications and medical devices used in healthcare.
> - Vendor risk assessments are time-consuming and costly, so only a few organizations are conducting risk assessments of all vendors.
> - Critical vendor management controls and processes are often only partially deployed or not deployed. [2]

The number of third-party vendors that handle sensitive data has grown as the volume and complexity of securing electronic medical data has increased. HDOs rely on third-party vendors for infrastructure, managed applications, and data management. Additionally, the complexity of managing third parties has increased. HDOs face the additional responsibilities and challenges of access management, change management, and data stewardship, even though they don't own the infrastructure or directly manage the resources involved. This poses a significant risk to the HDO; third parties have been responsible for almost half of all data breaches.[3]

1 RiskRecon, 2018. Third-Party Security Risk Management Playbook: A Study of Common, Emerging, and pioneering Capabilities and Practices, Retrieved from https://www.riskrecon.com/third-party-security-risk-management-playbook

2 Ponemon Institute LLC, 2019. The Economic Impact of Third-Party Risk Management in Healthcare, Retrieved from https://censinet.com/wp-content/uploads/2019/07/Ponemon-Censinet-Survey-Report-third-party-vendor-risk-management-research-economic-impact-v2-1.pdf

3 Grant Thornton LLP, 2013. Third-Party Relationships and Your Confidential Data: Assessing Risk and Management

© Copyright 2022, Cloud Security Alliance. All rights reserved.

As the number of third-party vendors increases it is essential that HDOs develop and implement a comprehensive risk management program. An important part of risk management is risk rating their third-party vendors. Basing the risk rating on predetermined criteria allows the HDO to use the rating on an objective basis for identifying risk and comparing third parties from a risk perspective. This objectivity allows for a more effective evaluation of a third party's ability to maintain a control profile (a list of controls and how they are implemented) that meets the HDOs expectations.[4]

HDOs need to establish a formal and practical risk rating process that determines the risk assessment frequency and prioritizes the assessment detail and actions for those assessments. An effective risk rating must be based on documented parameters, including scoring against the defined risk tolerance and risk appetite of the HDO. It is essential that a pre-engagement risk rating is conducted for every potential third-party vendor to determine appropriate levels of oversight and set relevant expectations for continuous monitoring and assessment.

Compounding these challenges are federal requirements and continuously evolving state requirements for managing electronic protected health information (ePHI). The changes underscore the need to carefully select third-party vendors using risk-based criteria. Failing to assess risks inherent in these relationships and failing to implement effective monitoring controls can be costly in terms of potential penalties and damage to HDO's reputation. The challenge with the organization relying on third parties is determining if vendors hired to store, process, or transmit digitally protected health information have the processes and controls in place to secure data, sufficiently manage risk, and meet privacy and security requirements. It is advantageous to use a framework such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework to measure, monitor, and track third-party risk. The framework is a risk-based approach to managing cybersecurity risk. Framework measurement provides a basis for a strong, trusted relationship.[5] While the framework is primarily for cybersecurity, it can help provide information for measuring other forms of risk. This is particularly true with version 1.1, which includes cyber supply chain risk management.

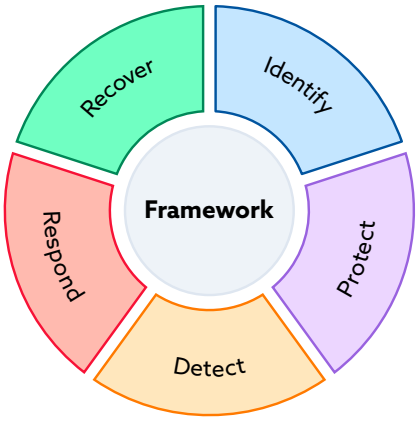

Figure 1 NIST Cybersecurity Framework

Oversight Processes, Retrieved from https://ahia.org/assets/Uploads/pdfUpload/Whitepaper.pdf

4 Shared Assessments, 2017. Risk Rating Third Parties: Optimizing Risk Management Outcomes, Retrieved from https://sharedassessments.org/wp-content/uploads/2017/10/SA_BP_RiskRating_FINAL_10OCT17.pdf

5 National Institute of Standards and Technology, 2017. Framework for Improving Critical Infrastructure Cybersecurity, Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Identify

Develop an organizational understanding of third-party risk and how to manage that risk. Identifying the risk is foundational for implementing an effective risk management framework. Understanding the business requirements for third-party vendors, the resources they supply, and how they support critical functions is essential for managing the risk. Identifying the third-party vendors and prioritizing them based on criticality enables the HDO to focus its efforts consistent with their risk management strategy based on business needs.[6]

Identify and Prioritize Third-Party Vendors

Implementing processes to identify new third parties and changes to existing third parties is the first step in developing a risk management program. You cannot manage your third-party vendors if you do not know who they are. Additionally, for HDOs to assess third-party vendors, they must understand how data is stored, processed, and transmitted within their organization. This level of understanding will help identify potential deficiencies in vendors' systems. Understanding the workflows at the data level provides HDOs with two primary benefits. First, they will understand the location of ePHI and have a comprehensive inventory of critical applications. Secondly, as workflows and technologies change, they can quickly understand the impact of those changes on the high-risk workflows.[7]

Once all third-party vendors have been identified, the HDO should risk-rank the vendors to identify the criticality of the vendor. Risk-ranking is "a standardized, scalable and repeatable due diligence procedure for identifying risks and categorizing third-party providers in light of those risks."[8] The risk rating should include the criticality of the services provided to the HDO and the data they are processing. Risk-rating third-party vendors is essential for a comprehensive risk management program. The risk rating should be based on predetermined criteria, allowing HDOs to use that rating to identify actual-versus-perceived risk. Also, HDOs can compare third parties from a risk perspective related to specific risk areas, like financial health, security controls, and resiliency.

6 National Institute of Standards and Technology, 2017. Framework for Improving Critical Infrastructure Cybersecurity, Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

7 Grant Thornton LLP, 2013. Third-Party Relationships and Your Confidential Data: Assessing Risk and Management Oversight Processes, Retrieved from https://ahia.org/assets/Uploads/pdfUpload/Whitepaper.pdf

8 Shared Assessments, 2017. Risk Rating Third Parties: Optimizing Risk Management Outcomes, Retrieved from https://sharedassessments.org/wp-content/uploads/2017/10/SA_BP_RiskRating_FINAL_10OCT17.pdf

© Copyright 2022, Cloud Security Alliance. All rights reserved.

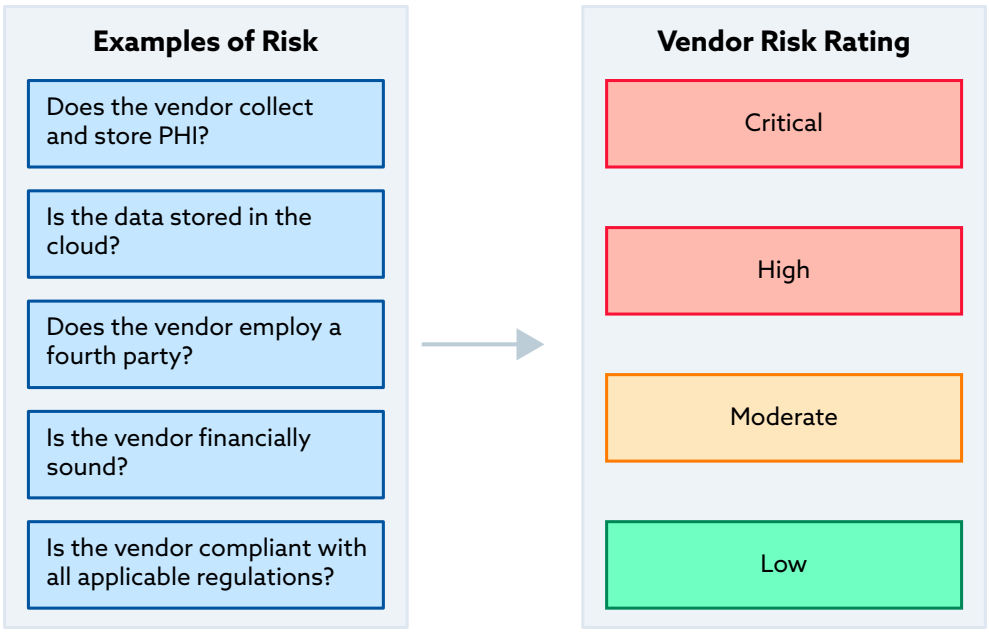

Figure 2 Example of third-party risk rating

Potential Risks from Third-Party Relationships

Outsourcing operations to third-party vendors has become a popular business strategy. It allows HDOs to save money and increase operational efficiency. As the role of third-party vendors expands, having vendor management processes in place becomes key to organizational success. Vendors have access to critical systems and PHI, so it is essential that HDOs monitor their cybersecurity risk to limit any potential threats they may pose.

HDOs face risk from many different third-party vendors, everything from food suppliers, software providers, medical devices, and day-to-day medical supplies, the HDOs depend on third parties to operate. Taking a risk-based approach to third-party vendor management requires HDOs to understand the different types of vendor risk. Knowing this allows HDOs to assess third-party risk and classify vendors based on their threat to the HDO.

There are numerous risks that may arise from the HDO's use of third parties. Some of the risks are associated with the underlying activity itself, like the risks faced by an institution directly conducting the activity. Some risks arise from, or are heightened by, the involvement of a third party. Failure to manage these risks can expose the HDO to regulatory action, financial loss, litigation, and reputation damage.[9]

9 Securityscorecard, 2020. Six Types of Vendor Risks That Are Important to Monitor, Retrieved from https://securityscorecard.com/blog/six-types-of-vendor-risk-that-are-important-to-monitor

© Copyright 2022, Cloud Security Alliance. All rights reserved.

The following are some of the risk types HDOs need to be aware of:

- Cybersecurity risk: The risk that the organization's data confidentiality, integrity, and/or availability is compromised due to deficiencies in a third party's cybersecurity controls. With cyber threats growing in sophistication and speed, it is important that HDOs monitor their vendor's cybersecurity posture.[10]
- Reputational: The risk that the HDO's brand reputation will be negatively impacted should an incident occur involving a third-party. Some of the ways third-party vendors can harm your reputation include:
  - Interactions that are not consistent with company standards
  - Loss or disclosure of customer information due to negligence or data breach
  - Violations of laws and regulations
- Compliance risk: The risk that arises from violations of laws, regulations, and internal processes that your organization must follow to conduct business. The laws that apply to each organization will vary by sector and country. However, there are some common regulations that span industries and countries, such as GDPR and PCI DSS. [11]
- Privacy risk: The risk that personal data shared with a third-party is accessible without authorization. The risk to privacy can be also correlated to the compliance risk. For example, the vendor that stores supply-chain data is hacked, revealing sensitive information about the companies the HDO does business with.[12]
- Operational risk: Third-party operations are intertwined with HDO operations, so when vendors cannot provide their services as promised, HDOs are usually unable to perform daily activities. An example is when a vendor-supplied system has an issue that causes it to go offline for a significant period of time. This could impact the HDO's ability to continue providing care at the same level as they normally do.
- Strategic risk: This risk arises when vendors make business decisions that do not align with the HDOs strategic objectives. An example is when a vendor the HDO relies on is bought by another company, and they feel the product the HDO depends on is not in their future plans and discontinue it.
- Financial: The risk that a third party could damage the organization's revenue. An example is if a pharmaceutical company has a drug used for specific treatments, and it is recalled. This can cause both a financial loss and a patient safety issue.

There are numerous types of risks posed by third parties. These are just some of them. The HDO should develop and implement a scalable third-party risk management program to manage all types of third-party risks. Once the risk is identified, the HDO should conduct a risk assessment, treat the risk, monitor the risk, and respond to issues.[13]

10 OneTrust Vendorpedia, 2021. Managing Third Parties: Identifying and Mitigating Privacy Risks, Retrieved from https://www.vendorpedia.com/blog/mitigating-privacy-risks/

11 Securityscorecard, 2020. Six Types of Vendor Risks That Are Important to Monitor, Retrieved from https://securityscorecard.com/blog/six-types-of-vendor-risk-that-are-important-to-monitor

12 OneTrust Vendorpedia, 2021. Managing Third Parties: Identifying and Mitigating Privacy Risks, Retrieved from https://www.vendorpedia.com/blog/mitigating-privacy-risks/

13 Securityscorecard, 2020. Six Types of Vendor Risks That Are Important to Monitor, Retrieved from https://securityscorecard.com/blog/six-types-of-vendor-risk-that-are-important-to-monitor

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Protect

The HDO develops and implements safeguards to ensure the delivery of critical services. Protect, supports the ability to limit the impact of potential events. Included in Protect are assessments. Key among assessments is the risk assessment. In addition to the risk assessment, the HDO should require the third-party vendor to complete a security questionnaire.[14]

Risk Assessment

The inability of HDOs to adequately assess third-party vendor risks is becoming costly to healthcare providers. According to the research, the yearly hidden costs of managing vendor risk is $3.8 million per HDO. The cost across the healthcare industry is $23.7 billion per year. The research indicates that 56 percent of HDOs have experienced a data breach introduced by one or more third-party vendors in the last two years.[15] Working with third-party vendors involves risk. HDOs have critical information that they do not want to lose. A risk assessment is used to determine the chances of an attack against the third-party vendor and the potential impact a cyberattack could have on its reputation, finances, and business health. It also helps the HDO understand and plan to prevent attacks on their organization. Additionally, a risk assessment can provide information that can help mitigate the risk or recover from an incident.

Given the cost and the number of breaches, HDOs need to conduct a comprehensive risk assessment for their third-party vendors.

Risk Analysis

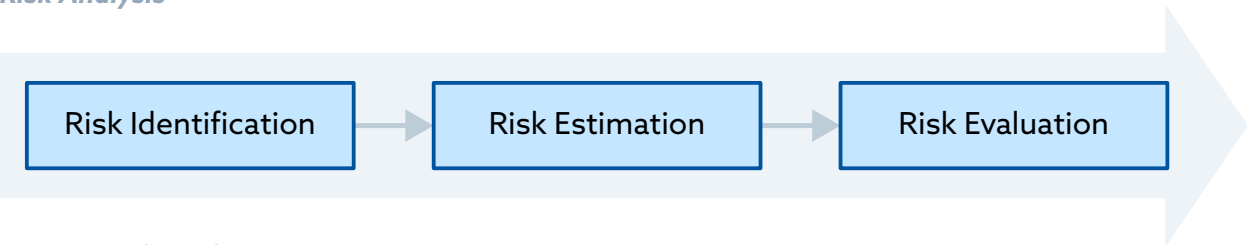

Figure 3 Risk Analysis

Before HDOs can assess the risks associated with third-party vendors, they must understand how data resides and moves within their organizations. Who processes information and how data is collected, transmitted, and stored? Understanding the workflows at the data level provides HDOs with a two-fold benefit: first, they can identify the location of ePHI and have a comprehensive inventory of critical applications. And second, as workflows change and technologies are replaced with new applications, they will be able to understand the impact of those changes on the high-risk workflows and whether the changes have implications for patients and the organization.[16]

14 National Institute of Standards and Technology, 2017. Framework for Improving Critical Infrastructure Cybersecurity, Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

15 College of Healthcare Information Management Executives, 2019. Ponemon Institute and Censinet Find Third-Party Risk Costs the Healthcare Industry $23.7 Billion a Year, Retrieved from https://chimecentral.org/ponemon-institute-and-censinet-find-third-party-risk-costs-the-healthcare-industry-23-7-billion-a-year/

16 Grant Thornton LLP, 2013. Third-Party Relationships and Your Confidential Data: Assessing Risk and Management Oversight Processes, Retrieved from https://ahia.org/assets/Uploads/pdfUpload/Whitepaper.pdf

© Copyright 2022, Cloud Security Alliance. All rights reserved.

A defined risk assessment process is necessary to guide the organizational process. The process needs to be built on a recognized industry standard, ISO, NIST, or HITRUST. The following are some capability practices the HDO should consider:

- Classify your vendors. Develop a method for classifying third-party vendors and assign each vendor a risk rating.
- Set a third-party assessment frequency and scope based on inherent risk rating. Third-party risk assessment is not a one-time process, it requires continuous monitoring and reassessment.
- Conduct third-party assessments using a recognized standard. Share the assessment with both the vendor and internal stakeholders. Ensure the vendor is accountable for addressing issues and record assessment results in a risk register.
- In addition to risk, assess for performance.
- Assess for financial risk
- Include business continuity risk; third-party can be a business continuity risk if they interrupt the HDOs.[17]

Developing an effective risk assessment process will positively affect the effectiveness and efficiency of the HDOs ethics and compliance program. Additionally, it will aid in protecting the HDO's critical data from exposure.

Security Questionnaire

The HDO should create a baseline security questionnaire. This could be a spreadsheet with security questions requiring responses, supporting artifacts, or a very detailed multipage document.

The questionnaire should cover a couple of key requirements:

A "scoring" mechanism to differentiate vendors and create the underpinning for differential policy applications. For example, a low-scoring organization may not have unsupervised remote access.

In addition, ask for one of the following:

- HITRUST certification
- SOC 2 report
- Third-party assessment against a recognized standard, such as the NIST CSF
- A completed questionnaire on internal security controls[18]

17 Ogden, M., 2020. 9 Tips Best Practices for Third-Party Risk Assessments, Retrieved from https://www.navexglobal.com/blog/article/third-party-risk-assessment-nine-tips/

18 Langston, F., 2021. Third Party Risk Management for Healthcare Cybersecurity, Retrieved from https://www.criticalinsight.com/resources/news/article/third-party-risk-management-for-healthcare-cybersecurity

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Risk Treatment

Once the HDO has identified and defined the risk, they must make sure they effectively manage to mitigate the risks. Risk mitigation requires steps to minimize the vulnerability of a third-party vendor to future threats. Creating a risk mitigation strategy for a third-party vendor can be a large time-consuming task. The identification and mitigation of risks require a well-established risk management program.

There are several different types of risk treatment options. You can break risk treatment options down into four types:

- **Avoid:** If a risk is deemed too high, you simply avoid the activity that creates the risk.
- **Transfer:** Risk transfer is when you transfer the risk you take to another party, such as an insurance company.
- **Reduce:** Risk reduction is a crucial step for processes or activities not avoidable, and where risk is transferable to another party.
- **Accept:** There is no option but to accept the risk for some processes and activities for a specified period of time.

Note that risk treatment options, with the exception of avoidance, do not reduce risk to zero. In many cases, there is a residual risk that must also be considered.[19]

Once the HDO decides how to treat the risk, they need to develop and implement a mitigation plan. A mitigation plan is used to reduce the severity of the identified risks and/or remediate them. Not all risks are created equal, The HDO must focus on the most important ones, the high-risk ones. This is where you move from theory to practice. Now, it's time to show some concrete results.

The purpose of the Risk Treatment Plan is to define exactly who will implement each control, in what timeframe, and with what budget. The information provided in a treatment plan should include:

- The reasons for selecting the treatment options, including expected benefits
- Who is accountable for approving the plan, and who is responsible for implementing it
- The actions proposed
- Resource requirements, including contingencies
- Performance measures and constraints
- Reporting and monitoring requirements
- Timing and schedule[20]

19 Infosec, 2018. Risk Treatment Options, Planning and Prevention, Retrieved from https://resources.infosecinstitute.com/topic/risk-treatment-options-planning-prevention/

20 Kolomiyets, T., 2017. Risk Treatment Process, Retrieved from https://statswiki.unece.org/display/GORM/4.2+Risk+treatment+process

© Copyright 2022, Cloud Security Alliance. All rights reserved.

When selecting new controls, there are basically four types of controls:

- The HDO can define new rules: rules are documented through plans, policies, procedures, and instructions.
- The HDO can implement technology: for example, backup systems, disaster recovery locations for alternative data centers, etc.
- The HDO may also have to change the organizational structure: they may need to introduce a new job function or change the responsibilities of an existing position.[21]
- The HDO may also have to enforce special legal commitments through the signed agreement with the third-party vendor.

The following are some steps the HDO can take:

- Identify asset ownership for each third-party service or tool in the inventory.
- Create and periodically review third-party service level agreements (SLAs) and Business Associates Agreements (BAA).
- Establish a channel for communicating threats and risks to the third party.
- Construct risk profiles for every third-party vendor. A risk profile provides an overall impact to the HDO (e.g., revenue, services, security, etc.) in case of an incident.
- Implement mitigating controls for securing third-party entry and exit points.
- Devise a remediation activity timeline for each risk identified during the assessment phase (e.g., threat modeling, application penetration testing, and source code analysis).
- Audit security controls implemented by the third-party vendor for the HDOs data. Data segregation with other organizations is important in case of a breach.
- Examine access to systems from third-party vendors.[22]

Residual risk is all the risk that cannot be completely mitigated. It is important that the HDO document third-party risk attributes and track them in the risk registry. Tracking third-party risks, including their inherent risks and business context, is required to manage third-party risks. Tracking risk is necessary to understand third-party residual risk.[23]

21 Kosutic, D., 2022. What is risk management, and why is it important, Retrieved from https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/

22 Infosec, 2018. Risk Treatment Options, Planning and Prevention, Retrieved from https://resources.infosecinstitute.com/topic/risk-treatment-options-planning-prevention/

23 RiskRecon, 2018. Third-Party Security Risk Management Playbook: A Study of Common, Emerging, and pioneering Capabilities and Practices, Retrieved from https://www.riskrecon.com/third-party-security-risk-management-playbook

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Detect

Detect is developing and implementing the appropriate control and activities to identify cybersecurity events. Detect controls enable timely discovery of events and incidents.[24]

Monitoring

The HDO should maintain an up-to-date understanding of their third-party risk by establishing a continuous monitoring program. Continuous monitoring is a tool for HDOs to improve their cyber third-party risk management programs. Adding an ongoing view of the vulnerabilities that vendors expose to the internet can help HDOs validate the answers they've received from annual security questionnaires. More importantly, HDOs can start to institute proactive governance practices based on empirical, continuous evidence of risk.[25]

Attestation-based assessments tell you what investments third parties have made in risk management. Continuous surface security assessment data objectively tells you how well they implement and operate their program. Continuous monitoring allows the HDO to develop an understanding of their third-party risk.[26]

There are numerous benefits to establishing a continuous monitoring program. The following are just a few. Continuous monitoring:

- Enables a proactive approach through real-time insight into your vendors
- Provides objective context to prevent human error and inaccuracies
- Saves time and resources, as opposed to conducting manual assessments that are slow and costly
- Allows for easy customization. Using automation and data intelligence, assessments can be tailored to the vendor, industry, or compliance need
- Allows you to focus only on the highest risks[27]

24 National Institute of Standards and Technology, 2017. Framework for Improving Critical Infrastructure Cybersecurity, Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

25 RiskRecon, 2020. 10 Steps to Incorporating Continuous Monitoring into Your Third-Party Risk Management Program, Retrieved from https://blog.riskrecon.com/incorporating-continuous-monitoring-into-your-third-party-risk-management

26 RiskRecon, 2018. Third-Party Security Risk Management Playbook: A Study of Common, Emerging, and pioneering Capabilities and Practices, Retrieved from https://www.riskrecon.com/third-party-security-risk-management-playbook

27 Booth, A., 2021 How Third Party Risk Management Ongoing Monitoring Enhances Vendor Monitoring, Retrieved from https://www.thirdpartytrust.com/blog/continuous-monitoring-enhances-third-party-risk-management/

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Another part of continuous monitoring that is often overlooked is threat intelligence. This requires monitoring hundreds of thousands of websites, forums, and marketplaces, or tracking malicious network activity for a long list of third-party partners. HDOs do not have the resources for this kind of monitoring. An intelligence service provider can assist by providing the skills and resources to draw information from sources across the internet, including websites, forums, and marketplaces on the open web and dark web, ransomware extortion sites, paste and dump sites, news sources, blogs, social media accounts, and threat intelligence databases.[28] Implementing continuous monitoring into your third-party risk management program will set the HDO up for a successful risk management program. Once implemented, continuous monitoring will enable the HDO to use verifiable and objective risk assessment information to establish risk-based management for third-party risk.

Risk Control

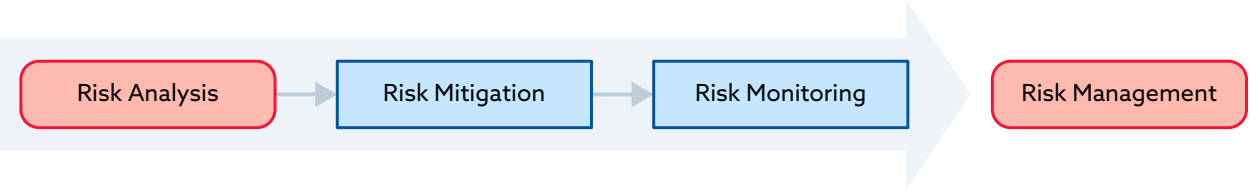

Figure 4 Steps in Risk Management

Respond

Respond requires the development and implementation of the activities regarding a detected cybersecurity event. This supports the ability to contain the impact of a potential event.[29]

Response

With third-party security incidents growing exponentially, companies must prepare for the worst. According to a recent survey, 83% of organizations have suffered a breach at the hands of a third party within the past three years. So, it's no wonder that security professionals quickly prioritize third-party security management. Since no two HDOs are exactly alike and no security incident is identical, responses to third-party security breaches will vary. That's why HDOs need to create an incident response playbook.[30]

Threat actors are exploiting technology vulnerabilities by targeting third-party vendors with direct access to many customer systems, rather than trying to compromise customer systems individually. While these breaches are responsible for allowing direct access to customer systems and data, HDOs also need to be aware of data shared externally with third parties. HDOs should understand

28 Recorded Future, 2021. Five Critical Third-Party Risks You Need to Monitor, Retrieved from https://go.recordedfuture.com/hubfs/ebooks/five-critical-third-party-risks-you-need-to-monitor.pdf?_hsmi=150939596&_hsenc=p2ANqtz-8Di7qWZfTCTCU7xa-ki-Kb5Jp9qMXfHvAJGaFmC9GR8BoKGlicGFuSEVaQEeH2WKtvmUD_-nlHPeN0M67689cxOdqk_Vqgcj0Pd297ozIsRrGOfXs

29 National Institute of Standards and Technology, 2017. Framework for Improving Critical Infrastructure Cybersecurity, Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

30 Panorays, 2021. The Third-Party Incident Response Playbook, Retrieved from https://resources.panorays.com/hubfs/assets/The_Third-Party_Incident_Response_Playbook.pdf?_hsmi=144386526&_hsenc=p2ANqtz-8HjpGzlb2sirYBeJXh8g2kHstm0a3uPy4iuFmralkslpn0e1nE4gbIMANQEsolDFeAX6aOtaczDk2DabT2mqD9Wv-RcQ

© Copyright 2022, Cloud Security Alliance. All rights reserved.

that state and federal data breach notification laws state responsibility for notifying individuals of a data breach are on the owner of the data, which in these cases is most often the HDO rather than the vendor. The vendor's only legal, and oftentimes financial, responsibility is to notify its customer organizations, and in turn, the customer organizations provide legal notification of a data breach to customers or employees.[31]

You've detected a breach in your third party; now what? The most critical thing is to limit the damage of the impact on your organization by activating your response playbook, which should include:

- Shut Off Access. Companies need to be able to shut off access to third parties affected by a cyberattack. HDOs should segregate third-party cyber assets from the rest of the network.
- Determine whether the third-party breach has affected your organization. If it has, your next step is to conduct forensic analysis to understand the extent of the incident and its impact.
- Assess liability from third-party involvement in breach, and check contract terms and conditions.
- Mitigating the damage. This can be done through additional security tasks, and tools to minimize any further incursion into your systems.
- Communicate to stakeholders what has happened, the impact, and your recovery plan.
- If the incident involves a breach of critical infrastructure, it must be reported to the Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) within 72 hours. This is a new requirement passed in March 2022.
- Conduct a root cause analysis to determine how to prevent the incident from recurring.
- Documenting the organization's response, what worked, what didn't, what improvements are needed, and the plan for implementing them next time.[32]
- Continue In-house. HDOs should have a plan for running services in-house in the event of an incident.

The HDOs incident response plan needs to be on paper and stored where employees can see and use the document. Additionally, as with all incident response plans, it must be tested and practiced ensuring it will work when needed. Be prepared.

31 Radke, B., Smith, C., Kalkat, N. and Schall, 2022. Tech Transactions & Data Privacy 2022 Report: Third-Party Data Incidents: Preparing and Responding as the Volume of Incidents Rise, The National Law Review, Volume XII, Number 95 retrieved from https://www.natlawreview.com/article/tech-transactions-data-privacy-2022-report-third-party-data-incidents-preparing-and

32 Ben-Ari, D, 2021. How the NIST Cybersecurity Framework Helps You Respond to a Vendor Breach, Retrieved from https://panorays.com/blog/how-nist-controls-help-you-respond-to-third-party-breaches/

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Recover

Develop and implement activities to maintain plans for resilience and to restore any capabilities or services that were interrupted by the event. This supports timely recovery to normal operations and reduces the impact of the cybersecurity event.[33]

After an incident is contained, the vendor needs to think through how to return to normal operations quickly. This includes restoring systems, the services associated with the vendor, and planning how to better protect them against future incidents. This is known as cyber resilience.[34]

The key focus of the HDOs third-party vendor incident recovery should be continuing patient care. The HDO should have a team identified to manage the recovery. Once an event has been identified, the team should actively engage vendors to identify alternative sourcing for the service provided by the affected vendor.[35] These sources should be engaged to provide essential services until full service can be restored.

There can be breaches that do not shut down services but disclose the HDO's data. The HDO needs to assess the breach's impact and determine what other activities need to be taken. Did the system contain sensitive data? If so, what are the reporting requirements? Do they have to notify the individuals whose data was compromised? Remember, there are reporting and notification requirements at the state and federal levels. The recovery playbook should have these requirements identified.

During the recovery effort, communication is very important. Information should be shared with both internal and external stakeholders. Within the organization as well as with customers and patients. The recovery is not just about getting back to business as quickly, and as safely as possible, it is also an opportunity to build confidence with your customers and patients. By communicating proactively and honestly with your customers and patients, and having a thought-out and detailed plan in place, you are building resilience, but also building business relationships.[36] Customers and patients want to know how you will protect their data going forward.

33 National Institute of Standards and Technology, 2017. Framework for Improving Critical Infrastructure Cybersecurity, Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

34 Ben-Ari, D, 2021. How the NIST Cybersecurity Framework Helps You Respond to a Vendor Breach, Retrieved from https://panorays.com/blog/how-nist-controls-help-you-respond-to-third-party-breaches/

35 National Institute of Standards and Technology, 2020. Case Studies in Cyber Supply Chain Risk Management, https://doi.org/10.6028/NIST.CSWP.02042020-5

36 Panorays, 2021. The Third-Party Incident Response Playbook, Retrieved from

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Additional Considerations

Cloud

Cloud computing is a rapidly growing challenge to the security of healthcare data. The benefits of cloud computing–access from anywhere, anytime, or on any device– can increase the difficulty of securing data. In healthcare, cloud computing can support numerous functions such as electronic medical records, prescription data, practice management, billing, and administration, just to name a few. Cloud computing offers many benefits to HDOs, and as a result, its use is rapidly growing within the healthcare sector.

With the benefits also come certain risks. The most difficult risk to assess comes from third-party vendors that subcontract with another cloud service provider. The result is a multilayered risk profile that presents complex issues for HDOs.

From an internal and IT security perspective, cloud computing risks can be divided into six areas:

- Data security and controls. As with other third-party custodians, providers must assess the strength of a cloud vendor's internal controls.
- Data transmission. Data may be transmitted over the Internet or wireless networks. HDOs must comply with all legal requirements when selecting cloud computing vendors. Remember to identify where the data is transmitted and stored.
- Multitenancy. This requires healthcare organizations to consider the possible commingling of data on shared hardware.
- Location. Moving data to the cloud means moving assets to a remote location that the healthcare provider doesn't control. Additionally, data may be stored outside of the U.S.
- Reliability. When relying on a shared resource such as the cloud, healthcare organizations face the risk that resources may not be available when needed.
- Sustainability. HDOs should determine the adequacy of a cloud provider's disaster recovery, and business continuity plans to understand how operations will continue if the cloud is out of service. [37]

When determining if they use a third-party vendor in the cloud, the HDO needs to ensure the proper assessment has been completed. While most cloud providers are reluctant to allow customers to assess their security controls directly, there are things the HDO can do. The HDO should require the vendor to have a Security Trust Assurance and Risk (STAR) registry. The STAR registry should be level 2, which requires third-party certification. Another certification the HDO can use is the Federal Risk and Authorization Management Program (FedRAMP), which is tailored to the NIST 800-53 controls.

37 Grant Thornton LLP, 2013. Third-Party Relationships and Your Confidential Data: Assessing Risk and Management Oversight Processes, Retrieved from https://ahia.org/assets/Uploads/pdfUpload/Whitepaper.pdf

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Additional security measures the HDO should require are:

- Multifactor authentication
- Data encryption, both at rest and in transit
- Federated access control includes adaptive access and identity proofing
- HDOs develop and implement data security policies to manage the activities of their users in the cloud environment[38]

Healthcare cloud security is a concern due to the possibility of third-party access to PHI shared and stored in the cloud. Therefore, HDOs must seek measures such as authentication, encryption, and revoking unauthorized access to manage the cloud data security risks.

Automation

HDOs have more third-party relationships than ever before. Keeping up with the dynamic landscape of risk and myriad regulations with each third-party vendor is cumbersome. HDOs must rely on automation to manage their third-party risk to keep up. An automated approach to third-party risk management is a critical risk mitigation tool.

Incorporating automation allows HDOs to lower their risk of successful attacks and improve performance in their third-party ecosystem.[39]

The following are four key benefits of automating your third-party risk management screening and monitoring:

- Efficiency. An automated program allows for efficient evaluation times, controlled processes, consistent workflows, and accurate documentation.
- Transparency. By screening and monitoring the records of all third parties, an HDO can respond to actual risk. A key part of an automated risk-based program is using data appropriately and applying resources to mitigate risk better.
- Organize and Categorize Your Policies. Categorize documents by any structure you use to delineate access to your documents. The structure should be searchable.
- Immediate Notification. An automated program can report violations and risks immediately.[40]

Integrating automation into your third-party risk management program may seem difficult, but given the growing complexities in accurately collecting and screening third-party data and the need for deeper due diligence, there is no other choice but to mitigate risk while reducing costs.[41]

38 Health and Human Services Cybersecurity Program, 2021. Threats in Healthcare Cloud Computing, Retrieved from https://www.hhs.gov/sites/default/files/threats-in-healthcare-cloud-computing.pdf

39 Bitsight, 2019. How automation is changing risk management, Retrieved from https://www.bitsight.com/sites/default/files/migration/documents/How%2520Automation%2520is%2520Transforming%2520Third-Party%2520Risk%2520Management%2520-%2520White%2520Paper.pdf

40 NAVEX, 2017. Definitive Guide to Third-Party Risk Management: How to Successfully Mitigate Your Organization's Third-Party Risk, Retrieved from https://www.navexglobal.com/en-us/resources/definitive-guides/definitive-guide-third-party-risk-management?RCAssetNumber=1880

41 Alster, B., 2019. Why Automation is Key to a Successful Risk Program, Retrieved from https://www.dnb.com/perspectives/corporate-compliance/automate-third-party-risk-management-programs.html

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Track & Improve Your Program's Effectiveness

Positioning risk to the HDO in the context of the mission, strategy, and objectives is the first step in making sure that activities add value to the overall risk management process. Pairing a risk-based approach with a strategic view enables communication and clarification of which risks have the highest potential to prevent the HDO from meeting its intended objectives and mission.

If you want to ensure that the HDO is managing the risk that has the most relevance to the HDO, the following are some things to think about for improving HDO's risk management process:

- Periodically revisit the CSF core functions (identify, protect, detect, respond, and recover) to understand if the functions implemented are efficient and effective.
- Is risk management a normal part of the HDOs operations, building risk identification into standard work procedures? Track progress of risk treatment activities against plans to get started with metrics.
- Evaluate risk activities to ensure that the most important third-party vendors are in scope. Some HDOs start with high-value assets that support the most critical business lines or critical services.
- Integrate the planning of risk management activities with the audit and compliance planning cycle. Often, there is an economy in collecting data once and using them to satisfy multiple information needs.

The main drivers for risk management are the need to improve decision-making in the HDO, align risk management resources to address the risk, and ensure that value is created by maintaining risk within acceptable tolerances and appetites.[42]

Measuring effectiveness is often unique to each HDO based on its business model, its geographic location, and the type of third parties engaged. There are multiple ways to measure the effectiveness of your program:

- The scalability of your solution
- The speed and accuracy of onboarding new third parties
- The consistency and actionability of your reporting
- The time and costs associated with remediation and monitoring alerts
- The ability to more accurately identify third-party characteristics that represent increased risk to your organization

The ability to manage better, or mitigate, associated risks
Ultimately, when you review your program performance, you must consider the initial risk assessment and where you are in relation to that.[43]

42 Young, L., 2019. Tips for Improving the Risk Management Process, Retrieved from https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2019/volume-8/tips-for-improving-the-risk-management-process

43 NAVEX, 2017. Definitive Guide to Third-Party Risk Management: How to Successfully Mitigate Your Organization's Third-Party Risk, Retrieved from https://www.navexglobal.com/en-us/resources/definitive-guides/definitive-guide-third-party-risk-management?RCAssetNumber=1880

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Conclusion

The increased use of third-party vendors for applications and data processing services is a business model that is likely to continue, especially as HDOs find it necessary to focus limited resources on core organizational objectives and contract out support services.[44]

An effective third-party risk management program is essential. Not only can the HDO more confidently engage with a growing network of vendors, suppliers, and distributors; but when done effectively, they can have a positive impact on the effectiveness and efficiency of the HDOs risk and compliance program.[45]

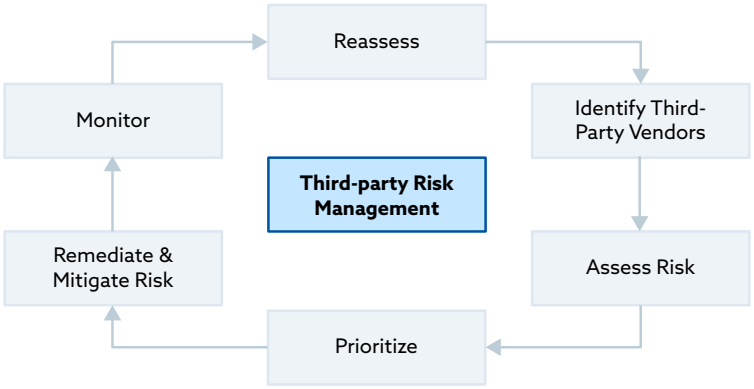

Figure 5 Third-Party Risk Management Program

The HDO should assess the risks against the business objectives and mitigate them by implementing security controls. Continuous monitoring of third-party assets, allows the HDO to detect and mitigate risks in near real-time.[46]

Additionally, remember there are multiple levels involved for some third-party vendors. The HDO must look at any vendors they use (fourth parties).[47]

HDOs have learned the hard way that the cost of confidential breaches can outweigh the expected cost efficiencies and other benefits associated with third-party custody of an HDO's confidential data.

44 Grant Thornton LLP, 2013. Third-Party Relationships and Your Confidential Data: Assessing Risk and Management Oversight Processes, Retrieved from https://ahia.org/assets/Uploads/pdfUpload/Whitepaper.pdf

45 Mehta, A., 2017. How to mitigate third-party security risks, Retrieved from https://www.synopsys.com/blogs/software-security/mitigate-third-party-security-risks/

46 NAVEX, 2017. Definitive Guide to Third-Party Risk Management: How to Successfully Mitigate Your Organization's Third-Party Risk, Retrieved from https://www.navexglobal.com/en-us/resources/definitive-guides/definitive-guide-third-party-risk-management?RCAssetNumber=1880

47 Cloud Security Alliance, 2022. Healthcare Supply Chain Cybersecurity Risk Management, Retrieved from https://cloudsecurityalliance.org/research/artifacts/

© Copyright 2022, Cloud Security Alliance. All rights reserved.

References

Alster, B., 2019. *Why Automation is Key to a Successful Risk Program*, Retrieved from https://www.dnb.com/perspectives/corporate-compliance/automate-third-party-risk-management-programs.html

Ben-Ari, D, 2021. *How the NIST Cybersecurity Framework Helps You Respond to a Vendor Breach,* Retrieved from https://panorays.com/blog/how-nist-controls-help-you-respond-to-third-party-breaches/

Bitsight, 2019. *How automation is changing risk management,* Retrieved from https://www.bitsight.com/sites/default/files/migration/documents/How%2520Automation%2520is%2520Transforming%2520Third-Party%2520Risk%2520Management%2520-%2520White%2520Paper.pdf

Booth, A., 2021. *How Third-Party Risk Management Ongoing Monitoring Enhances Vendor Monitoring,* Retrieved from https://www.thirdpartytrust.com/blog/continuous-monitoring-enhances-third-party-risk-management/

College of Healthcare Information Management Executives, 2019. *Ponemon Institute and Censinet Find Third-Party Risk Costs the Healthcare Industry $23.7 Billion a Year,* Retrieved from https://chimecentral.org/ponemon-institute-and-censinet-find-third-party-risk-costs-the-healthcare-industry-23-7-billion-a-year/

Cloud Security Alliance, 2022. Healthcare Supply Chain Cybersecurity Risk Management, Retrieved from https://cloudsecurityalliance.org/research/artifacts/

Grant Thornton LLP, 2013. *Third-Party Relationships and Your Confidential Data: Assessing Risk and Management Oversight Processes,* Retrieved from https://ahia.org/assets/Uploads/pdfUpload/Whitepaper.pdf

Health and Human Services Cybersecurity Program, 2021. *Threats in Healthcare Cloud Computing,* Retrieved from https://www.hhs.gov/sites/default/files/threats-in-healthcare-cloud-computing.pdf

Infosec, 2018. *Risk Treatment Options, Planning and Prevention,* Retrieved from https://resources.infosecinstitute.com/topic/risk-treatment-options-planning-prevention/

Kosutic, D., 2022. *What is risk management, and why is it important,* Retrieved from https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/

Langston, F., 2021. *Third-Party Risk Management for Healthcare Cybersecurity,* Retrieved from https://www.criticalinsight.com/resources/news/article/third-party-risk-management-for-healthcare-cybersecurity

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Mehta, A., 2017. *How to mitigate third-party security risks,* Retrieved from https://www.synopsys.com/blogs/software-security/mitigate-third-party-security-risks/

National Institute of Standards and Technology, 2017. F*ramework for Improving Critical Infrastructure Cybersecurity*,
Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology, 2020. *Case Studies in Cyber Supply Chain Risk Management,* https://doi.org/10.6028/NIST.CSWP.02042020-5

NAVEX, 2017. *Definitive Guide to Third-Party Risk Management: How to Successfully Mitigate Your Organization's Third-Party Risk,*
Retrieved from https://www.navexglobal.com/en-us/resources/definitive-guides/definitive-guide-third-party-risk-management?RCAssetNumber=1880

Ogden, M., 2020. *9 Tips Best Practices for Third-Party Risk Assessments,* Retrieved from https://www.navexglobal.com/blog/article/third-party-risk-assessment-nine-tips/

OneTrust Vendorpedia, 2021. *Managing Third Parties: Identifying and Mitigating Privacy Risks,*
Retrieved from https://www.vendorpedia.com/blog/mitigating-privacy-risks/

Panorays, 2021. *The Third-Party Incident Response Playbook,*
Retrieved from https://resources.panorays.com/hubfs/assets/The_Third-Party_Incident_Response_Playbook.pdf?_hsmi=144386526&_hsenc=p2ANqtz-8HjpGzlb2sirYBeJXh8g2kHstm0a3uPy4iuFmralkslpn0e1nE4gbIMANQEsolDFeAX6aOtaczDk2DabT2mqD9Wv-RcQ

Ponemon Institute LLC, 2019. *The Economic Impact of Third-Party Risk Management in Healthcare,*
Retrieved from https://censinet.com/wp-content/uploads/2019/07/Ponemon-Censinet-Survey-Report-third-party-vendor-risk-management-research-economic-impact-v2-1.pdf

Radke, B., Smith, C., Kalkat, N. and Schall, 2022. *Tech Transactions & Data Privacy 2022 Report: Third-Party Data Incidents: Preparing and Responding as the Volume of Incidents Rise,* The National Law Review, Volume XII, Number 95 retrieved from
https://www.natlawreview.com/article/tech-transactions-data-privacy-2022-report-third-party-data-incidents-preparing-and

Recorded Future, 2021. *Five Critical Third-Party Risks You Need to Monitor,*
Retrieved from https://go.recordedfuture.com/hubfs/ebooks/five-critical-third-party-risks-you-need-to-monitor.pdf?_hsmi=150939596&_hsenc=p2ANqtz-8Di7qWZfTCTCU7xa-ki-Kb5Jp9qMXfHvAJGaFmC9GR8BoKGlicGFuSEVaQEeH2WKtvmUD_-nlHPeN0M67689cxOdqk_Vqgcj0Pd297ozIsRrGOfXs

RiskRecon, 2018. *Third-Party Security Risk Management Playbook: A Study of Common, Emerging, and pioneering Capabilities and Practices,*
Retrieved from https://www.riskrecon.com/third-party-security-risk-management-playbook

© Copyright 2022, Cloud Security Alliance. All rights reserved.

RiskRecon, 2020. *10 Steps to Incorporating Continuous Monitoring into Your Third-Party Risk Management Program,* Retrieved from https://blog.riskrecon.com/incorporating-continuous-monitoring-into-your-third-party-risk-management

Securityscorecard, 2020. S*ix Types of Vendor Risks That Are Important to Monitor,* Retrieved from https://securityscorecard.com/blog/six-types-of-vendor-risk-that-are-important-to-monitor

Shared Assessments, 2017. *Risk Rating Third Parties: Optimizing Risk Management Outcomes,* Retrieved from https://sharedassessments.org/wp-content/uploads/2017/10/SA_BP_RiskRating_FINAL_10OCT17.pdf

Young, L., 2019. *Tips for Improving the Risk Management Process*, Retrieved from https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2019/volume-8/tips-for-improving-the-risk-management-process

© Copyright 2022, Cloud Security Alliance. All rights reserved.