RISK

MANAGING THIRD-PARTY RISK

Cyberrisk Practices for Better Enterprise Risk Management

OneTrust Vendorpedia™
THIRD-PARTY RISK SOFTWARE

ISACA®

CONTENTS

4 **Introduction**

5 **Key Definitions for Third-party Risk**

5 **Third-party Governance**

5 / Third-party Management Roles

6 / Enterprise Procurement

6 / Third-party Data Handling Agreement

6 / Third-party Metadata

7 **Third-party Risk Assessment Process**

7 / Third-party Risk Triage (Inherent Risk Assessment)

8 / Third-party Data Classification

9 / Third-party Administrative Assessment

9 / Contract

9 / Penetration Testing (Pentest) Results

9 / Accreditation, Certifications and Other External Audit Reports

10 / Internal Audit Reports

10 / Policy Review

10 / Data Flows

11 / Open Issues (From Previous Assessments)

11 / Incidents

11 / Control Questionnaire

11 / Third-party Onsite Assessments

12 / Technology-aided Reviews

13 **Risk Analysis**

14 **Threat Modeling**

15 **Determining Risk Ratings**

16 **Assessment Closeout and Ongoing Monitoring**

17 **Conclusion**

18 **Acknowledgments**

ABSTRACT

Many enterprises rely on third-party vendors to help facilitate the delivery of products and services to their customers. However, these relationships come with risk. Data privacy must be a top priority in these relationships. Ultimately, the enterprise is accountable for the protection of its data; therefore, enterprise vendor risk management must ensure a safe and healthy relationship with suppliers. Enterprises must also have sound governance, which includes business and technical requirements to ensure due diligence in the protection of the enterprise and its customers' data. A robust third-party risk management program includes the integration of risk management processes into enterprise and IT business practices. This white paper provides you with best practices to help manage enterprise third-party risk.

Introduction

End-of-year holiday shopping is critical for retail businesses. As a result, there is a lot of emphasis on ensuring that business operations are working flawlessly, including an enterprises' credit card processing systems. During this critical time of year in 2013, a landmark third-party cyberrisk incident occurred at a large US-based retailer. A phishing campaign infected the retailer's heating, ventilation and air conditioning (HVAC) contractor with the Citadel trojan, which enabled attackers to gain full control over the contractor's systems. After a few lateral moves and pivoting techniques, the hackers discovered that this HVAC contractor had access to the retailer's billing and project management systems.[1]

Like many enterprises, the retailer's network segmentation was limited, and attackers exploited the lack of tollgates to traverse the retailer's network and locate some point-of-sale (POS) systems. The attackers installed the BlackPOS malware, which steals credit card data, on some of the retailer's integrated Windows®-based POS terminals. The attackers did a trial run during one of the busiest holiday shopping weekends on a few POS terminals and were pleased with the results. Over the next two days, before the end of November, the attackers successfully deployed the BlackPOS malware to a majority of stores and were actively collecting credit card data.[2]

This data breach became one of the largest on record, affecting around 100 million customers and costing the retailer over US$200 million. Much of the cost reflected reimbursements to issuing banks for replacing compromised credit cards and settling class action lawsuits from the breach.[3]

The breach established a dominant narrative for many business executives considering their enterprises' third-party risk; it left many wondering which third parties on their networks could cause a similar breach. The link between the retailer and its HVAC third party allowed clever adversaries to infiltrate the retailer's network, infect the retailer's systems and extract millions of records. The breach not only raises questions about how much an enterprise really knows about its third parties, the controls that they have in place, the effectiveness of the controls and the nature of risk acceptance in third-party contracts—it also creates fear about what can go wrong.

The breach established a dominant narrative for many business executives considering their enterprises' third-party risk; it left many wondering which third parties on their networks could cause a similar breach.

Enterprise executives are concerned about the lack of complete information on third-party vendors, data and systems that the enterprise accesses in the course of vendor engagements. This concern has driven many enterprises to consider third-party risk management one of the top priorities of their cybersecurity programs, because customers do not regard the enterprise as a separate entity from its third parties. Therefore, **third-party risk is enterprise risk**.

This white paper provides third-party risk best practices covering governance issues (such as contracting, procurement and metadata mapping), forms of third-party risk assessment (including administrative, onsite and technology-based assessments), integration into a risk analysis process, and closeout and monitoring activities. By following the guidelines in this white paper, an enterprise can improve its third-party risk management program and avoid headlines for a third-party breach.

[1] Krebs, B.; "Target Hackers Broke in Via HVAC Company," KrebsonSecurity, 5 February 2014, https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
[2] Krebs, B.; "A First Look at the Target Intrusion, Malware," KrebsonSecurity, 15 January 2014; https://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/
[3] Consumer Bankers Association (CBA), "Cost of Target Data Breach Exceeds $200 Million," 18 February 2014, https://www.consumerbankers.com/cba-media-center/media-releases/cost-target-data-breach-exceeds-200-million

Key Definitions for Third-party Risk

This white paper uses the term third party to denote an enterprise that is hired by another enterprise to accomplish the terms set forth in a legal contract. Third party is synonymous with vendor. The term fourth party indicates any third party of a third party.

Some enterprises—including government-sponsored enterprises (GSEs)—provide obligatory access to certain governmental or quasi-governmental organizations. For simplicity, these organizations are treated here like third parties, although not all the same controls and ability to influence exist. Also, during any merger and acquisition, it is often prudent to treat the parties as third parties to each other when conducting due diligence, until the merger or acquisition is complete.

This white paper uses terminology from the Open FAIR™ standard[4] to ensure clear communication of terms and consistent use of concepts in enterprise risk calculation.[5]

Third-party Governance

The importance of having a complete list of all third parties of an enterprise cannot be overstated. There is no worse scenario than receiving notification from an unknown third party that they experienced a breach affecting the enterprise. The Center for Internet Security® (CIS®) top 20 critical security controls (CSCs)—also known as CIS Controls™ or the SANS™ top 20[6]—cite inventory of approved hardware and software as the first two security controls. No third party is reducible to hardware or software—but inventory management for enterprise third parties *is* covered in these critical controls. To ensure accuracy of third-party lists, the key control is clearly defining enterprise roles responsible for each aspect of the third-party engagement life cycle.

Third-party Management Roles

Typically, a third party provides services or products for one person, who is often referred to as the business owner in the enterprise. This role defines duties or deliverables from the third party, and often pays the third-party fees. This very critical role requires deep understanding of the third party's function and/or actions on behalf of the enterprise, the data that the third party needs, and the general level of access necessary to execute the job. The business owner role commands the leverage with the third party to compel it to take security seriously. This leverage often results in compelling remediation activities and responses to any control deficiencies that might be uncovered. A business owner tends to own the contract and often signs it, and initiates contract modifications that are necessary to support increased security posture.

For large enterprises that may have several contracts with a single third party, the relationship manager role often has overall accountability for the entirety of the third-party relationship. This role is similar to the business owner, but requires greater understanding of the overall third-party scope of work. The relationship manager must have sufficient expertise and authority commensurate with the risk and complexity of goods and services offered by the third party. The relationship manager's primary vehicle for control is the master services agreement (MSA). This legal agreement documents the terms and conditions under which the enterprise and the third party interact and details overall control paradigms that are uniform across all subordinate contracts. The MSA often mandates

[4] The Open Group®, Open FAIR™ (Factor Analysis of Information Risk), https://publications.opengroup.org/editors-picks/open-fair
[5] The Open Group, *Risk Taxonomy (O-RT) Version 2.0*, 18 October 2013, https://publications.opengroup.org/c13k
[6] Center for Internet Security, "CIS Controls™," https://www.cisecurity.org/controls/; Sans™ Institute, "The CIS Critical Security Controls for Effective Cyber Defense," https://www.sans.org/critical-security-controls/

deployment of large-scale cybersecurity controls. Through the relationship manager, the enterprise must ensure that third parties have a written information security program (WISP) and business continuity plan (BCP) based on industry-recognized security frameworks.

The relationship manager must have sufficient expertise and authority commensurate with the risk and complexity of goods and services offered by the third party.

To ensure that a third party has access to all required IT resources in an enterprise, business owners and relationship managers often engage with internal technology partners who perform the critical role in service fulfillment and in limiting access to nonauthorized persons. This role often includes one or more technology professionals from different parts of the IT organization, including information security.

Many enterprises also have an administrative role that enables third-party procurement. This role encompasses procurement and accounting systems, and may gather approvals within the enterprise and/or request specific technology access to enable the third party to accomplish its roles. These procurement professionals have a comprehensive view of the entirety of an enterprise's third parties and recommend consolidation of third parties in certain areas to ensure there is adequate leverage to gain the best pricing possible.

The final role is the legal team, which includes the privacy team. Formally reviewing and approving legal language on behalf of an enterprise requires not only appropriate licensing to practice law on behalf of an enterprise, but also the ability to ensure that appropriate protections are in place to safeguard enterprise reputation and treasury. This role cannot provide appropriate subject matter expertise regarding the nature of the contract and the work to be done, so the business and technology professionals, including cybersecurity professionals, may need to participate in contract review to become familiar with the terms of the deal and to suggest edits where appropriate.

Enterprise Procurement

Enterprises differ in the ways they approach purchasing of third-party services. Some enterprises allow business and technology leaders to purchase whatever services they need, provided they execute those purchases through a central system or enterprise support group to ensure that the proper process is followed. Other enterprises restrict purchasing to a centralized procurement group that purchases services on behalf of the business and technology leadership teams. Centralization is critical in procurement to ensure a complete inventory of third parties. By applying the financial control of centralizing purchases, the information security team gains a complete inventory of third parties used throughout the enterprise. Centralizing purchases also holds business leaders accountable for ensuring that the appropriate technology connections are made for their third parties and enables technology partners to ensure that the connection requests they receive are for authorized third parties only. The third-party inventory should be structured and centrally stored in a way that supports reuse, appropriate access and (ideally) automated processing.

Third-party Data Handling Agreement

Managing third-party risk has a strong technology focus. For example, opening firewall ports to enable third-party access, provisioning virtual desktop infrastructure (VDI) and processing large data transfer requests are processes that should be accommodated only for third parties on the approved third-party list, and only when appropriate data handling agreements have been executed as part of the authorization. The agreements ensure that data are transmitted in the context of appropriate legal and privacy protections and proper information security controls.

Third-party Metadata

It is often useful to collect metadata about third-party engagements to support not only cyberrisk assessments, but also other types of assessment. For example, knowing

the data types and volumes that third parties store, process and transmit helps an enterprise understand the role of the third party. Tracking the country in which data are manipulated helps ensure compliance with data privacy laws and other legal and contractual obligations, and also helps the enterprise maintain current data-flow documentation—all essential information for assessing enterprise risk.

Ideally, metadata should be correlated with records of authorized third parties and stored in a central database that supports *ad hoc* queries. An enterprise could query the database for information, such as:

- Type of data elements that each third party accesses, including:
  - Tax identification numbers
  - Genetic information
  - Health billing codes
- Countries where a third party processes data or moves data
- Platforms for processing data, i.e., local computing resources or a cloud server (including, as applicable, the specific cloud)

The ability to query specific data elements that third parties access is critical to the third-party risk triage process.

Third-party Risk Assessment Process

The third-party risk assessment process ascertains the risk to the enterprise from engaging with a third party and the impact of that risk on enterprise objectives. Three assumptions can be made about the third-party risk assessment process:

- The enterprise always knows more about its own computing environment than about its third parties.
- Third-party responses to enterprise inquiries about security programs carry a necessary veil of abstraction to help safeguard the third party from undue harm, such as targeted attacks by insiders. This veil is similar to the one that an enterprise applies to its responses to security-program inquiries from customers; an enterprise provides high-level information about its security program, but rarely reveals specific information.
- Most enterprises have many third parties that may not require a security assessment. For example, office supply companies are not likely to pose an information security risk to an enterprise. A risk triage process is required to determine the appropriate level of engagement for each third party.

Third-party Risk Triage (Inherent Risk Assessment)

The triage process was created for battlefield injuries, to sort injured soldiers into groups based on the severity of their injuries, and it can provide a rough framework for the third-party risk triage process. Essentially, such triage activity was meant to sort soldiers roughly into three groups:

- Those who would live, regardless of what doctors did
- Those who would die, regardless of what doctors did
- Those who might live if they received immediate attention

A third-party risk triage process does not need to be quite so intense, but the same basic rules can apply. If an enterprise has limited resources to conduct third-party reviews, it can prioritize third parties based on risk, and ration resources to those third parties that should get the most attention to help stave off grave risk. The triage process—also called a third-party inherent risk assessment—groups third parties into three categories according to potential risk:

1. Third parties that receive no reviews (no further assessments)
2. Third parties that receive an administrative review, such as a questionnaire and/or a scan
3. Third parties that receive a significant review, such as an administrative review plus an onsite evaluation

To determine the inherent risk that a third party can pose, the enterprise evaluates third-party demographic data and the nature of the third-party relationship it has or will have. This evaluation necessitates understanding:

- Terms and conditions of the contract with the third party
- Criticality of third-party services or products relative to enterprise business objectives
- Volume and nature of data shared with the third party (which factors are of particular importance)

Control-based questions are delayed until later to allow for a pure evaluation of the risk that the third-party relationship poses to the enterprise. The risk triage questions focus on evaluating the two relevant parts of the risk equation:

- Frequency of loss events
- Magnitude of losses if they occur

The following sample questionnaire for third-party risk triage helps assess the potential for threat actors to cause loss and any related impact to data confidentiality, integrity and availability.

1. Does the use of this third party involve any external-facing systems (including cloud)?
2. Will this third party subcontract enterprise work to any fourth party, use offshore resources, or provide or consume data feeds to/from external partners?
3. Will the use of this third party introduce any net new technologies to the enterprise?
4. Will this third party introduce any new functions for an existing system?
5. How many records will this third party store, transmit or process, and of which type (e.g., tax identification numbers, credit cards, dates of birth, financial account numbers, driver license numbers, email addresses, health information and similar sensitive data)?
6. Will this third party have the ability to move money, make investments or otherwise commit money to be spent on behalf of the enterprise?
7. What is the business criticality of the systems in use or affected by this third party?
8. If the systems/services provided by the third party go offline, is the enterprise required to notify regulators or pay fines to its customers?
9. Is the enterprise required to produce and/or submit evidence of regular review of the systems affected by this third party to regulators and/or auditors?

This list represents common, basic questions that an enterprise may want to ask. An enterprise should develop new questions (and/or adapt the example) to suit its specific environment and needs. Some enterprises may include privacy-related questions to gain a better understanding of the nature of the relationship and, if appropriate, may refer the third party to a privacy group that will conduct or update a privacy impact assessment (PIA). The following basic privacy triage question can be used for that purpose:

10. Will this third party be asked to contact individuals or store their data for marketing purposes (browsing or online-interaction information, email, phone, mail, text, etc.)?

The third-party risk triage—combined with data classification, as discussed in the following section—should form the basis of an inherent risk assessment of enterprise third parties, so that the enterprise can undertake the appropriate level of formal risk assessment.

Third-party Data Classification

Many of the questions in the previous section cover the confidentiality, integrity and availability (CIA) triad[7] In order to document all data types used by a third party—a critical complement to the CIA factors—enterprises should develop a specific, dedicated data-classification questionnaire (which can be reused in other risk assessments). When answering data-classification questions, respondents ideally will not choose the data

[7] Regarding confidentiality, integrity and availability security triad, see Sundaram, J.; "The Benefits of the Statement of Applicability in ISMS Projects," *ISACA Journal*, 2017:3, https://www.isaca.org/Journal/archives/2017/Volume-3/Pages/the-benefits-of-the-statement-of-applicability-in-isms-projects.aspx.

classification directly—e.g., confidential or personally identifiable information (PII). Instead, the respondent will indicate the specific data elements that are in use; the questionnaire applies logic and derives the classification for them. For example, respondents select Social Security number, driver license number, health diagnostic codes or mental health records. These data types can be correlated with the appropriate category and classification labels (e.g., PII and confidential). This approach gives the enterprise the added benefit of an inventory of the data types in use by the enterprise and indicates to which third parties the data are being transmitted. This information is critical for compliance with certain privacy regulations and some customer contracts (for example, a contract may state that certain data types cannot be sent offshore). This inventory is also helpful if the third party incurs a data breach. One of the first questions that an enterprise may want to ask is, "What data do we have there?" Not having the answer to this question puts an enterprise at greater risk if a breach occurs.

Third-party Administrative Assessment

For third parties that fall into the first triage category—i.e., no further review—the only assessment requirement is to monitor the third parties to see if anything changes. An annual review of these third parties is recommended; business owners are responsible for accurate answers to the risk questions and should inform the enterprise if anything changes that brings the third parties into scope for further action.

For the second category—i.e., administrative assessment—a range of steps will help the enterprise gain comfort without sending staff to third-party offices for a review. The following subsections cover documentation that can be reviewed, along with key considerations for each category.

Contract

Reading the contract that is in place with the third party gives insight into the work the third party is contractually obligated to perform on behalf of the enterprise. Contracts can include the MSA and/or any other special project agreements that are in place, including, for example, statements of work (SOWs). The enterprise should verify that there is a right to audit clause; if no such clause exists, the enterprise may be very limited as to what it can do in the assessment.

Penetration Testing (Pentest) Results

The enterprise should ask the third party for detailed pentest results (although the enterprise may not be able to get them, or may receive only redacted or summary versions). If the enterprise does not receive pentest results, this fact is included in the issue management process. Pentest results are assurance, from either a third party conducting the pentest or the unbiased output of a software tool, that the systems are as secure as warranted. For any significant adverse findings from these results, the enterprise asks for assurance from the third party that the findings were resolved. Some third parties may share pentest reports, but only for external systems—e.g., those with external Internet Protocol (IP) addresses. Finally, it is important to know against which risk scenarios these kinds of controls protect (that is, against external attackers versus insiders).

Accreditation, Certifications and Other External Audit Reports

This assessment category includes a statement provided by an external auditor attesting to the third-party's state of security upon which the enterprise can rely—for example, an ISO 27001 registration, which can be verified on the issuing organization's website. It may also include:

- Statement on Standards for Attestation Engagements (SSAE) No. 16 reports
- Service Organization Control (SOC) type 1 or 2 reports
- Payment Card Industry Data Security Standard (PCI DSS) testing results

Some third parties have HITRUST® certification, while others get a generic statement from an external auditor regarding their adherence to standards, including:

- US National Institute of Standards and Technology (NIST), Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*[8]
- NIST, *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1[9]
- SANS™ CIS® Critical Security Controls (SANS Top 20)[10]
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) and associated regulations[11]
- Federal Information Security Management Act of 2002, Federal Information Security Modernization Act of 2014 (FISMA)[12]
- North American Electric Reliability Corporation (NERC) Reliability Standards[13]
- COBIT® 2019[14]

Whatever accreditations a third party offers, an enterprise examines carefully the scope statements therein. Some accreditations cover everything in the third party, while others are tailored to certain operations, physical locations or services. If these scopes or service levels do not align with the enterprise use cases for the third party, they are not relevant. New tools—called exchanges—aggregate third-party data, including security and privacy certifications and accreditations, recent incidents, and other relevant data, so that an assessor can quickly understand how data are protected without sending an assessment to the third party.

Internal Audit Reports

An enterprise should also ask the third party for copies of its internal audit reports. These reports represent an independent review of security, albeit not as reliable as if they came from an external auditor. The same caveats apply as in the accreditation section; the reports may be redacted and the enterprise should check the scope statements for applicability.

Policy Review

An enterprise should ask for copies of third-party security policies and standards. Because terminology differs between enterprises, it is best to ask for any security governance documents that dictate where security controls (technical, physical and administrative) are required. Some third parties are happy to share these documents with an enterprise (assuming a properly executed nondisclosure agreement). Other third parties refuse to share policy documents, arguing that it may compromise them or their other customers. Some third parties may restrict how they share—for example, by allowing an enterprise to view only a physical copy, but no digital copy. When an enterprise encounters pushback from a third party, the enterprise should ask for the written information security program (WISP) as required in the contract, and any high-level security statements approved by the third-party board of directors or other governance bodies. At the very least, an enterprise should have the third party attest that it has such governance documents in place, and that they cover key areas specific to the enterprise use of that third party (access control, business continuity, etc.).

Data Flows

An enterprise should ask the third party for data flow diagrams, which outline not only where enterprise data comes into the third party (data feeds, manual loading, etc.), but also into which systems data flow (including systems of any fourth parties). These diagrams give enterprises the most complete picture of what scope of controls is needed and where risk can be introduced.

[8] US National Institute of Standards and Technology, NIST Special Publication 800-53 Revision 4, April 2013, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[9] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, 16 April 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
[10] *Op cit* SANS™ Institute
[11] US Department of Health and Human Services, Health Insurance Portability and Accountability Act, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html
[12] US Department of Homeland Security, Federal Information Security Modernization Act, https://www.dhs.gov/cisa/federal-information-security-modernization-act
[13] North American Electric Reliability Corporation, https://www.nerc.com/pa/Stand/Pages/default.aspx
[14] ISACA, COBIT® 2019, USA, 2018, http://www.isaca.org/COBIT/Pages/default.aspx

Open Issues (From Previous Assessments)

If the enterprise has assessed the third party before, it reviews the work papers from the previous engagement, looking for follow-up activity and closure of findings in the interim. Lack of action can indicate lack of commitment to secure the third party's environment. The enterprise asks its business owners to sign off on any risk associated with third-party control deficiencies from this and any previous engagement.

Incidents

An enterprise should search the news for any incidents involving a third party and ask pointed and targeted questions about the incidents to ensure there is appropriate follow-up and that the enterprise is not exposed. There are many tools available that can search for this information and help to automate the process.

Control Questionnaire

An enterprise develops its own control questionnaire that allows it to gain assurance that proper controls are in place to protect the enterprise and its data and services. There are service providers that can assist with this questionnaire. As the Accreditation, Certification and Other External Audit Reports subsection touched on, there are many control frameworks to guide an enterprise, such as the Cloud Security Alliance® (CSA) Consensus Assessments Initiative Questionnaire (CAIQ)[15], Shared Assessments SIG[16], NIST 800-53[17] and ISO 27002[18].

Third-party Onsite Assessments

Third parties that fall into the third risk triage category—i.e., onsite assessment—warrant a more in-depth review, because there is significant risk to the enterprise if that third party were to fail in some way. An enterprise performs additional due diligence to ensure that a third party has done what any reasonable enterprise would do to ensure its data are protected. Third parties in this category undergo an administrative assessment and an onsite assessment.

An interviewing style should be cultivated to help third parties assessors understand some nonverbal responses that may be given to inquiries, how to interpret them and which questions can aid in gathering information.[19] The enterprise must be careful to not interrogate third parties, but simultaneously be thorough with its evaluation.

Onsite third-party assessments typically include an in-person review of items listed in the administrative assessment section, although that review typically happens ahead of time, and onsite discussion focuses on any documents or specific responses that are particularly revealing.

It is customary to have a data center walkthrough while conducting the onsite review. The walkthrough typically allows enterprise assessors to see physical controls and learn how the third party conducts itself when dealing with guests. Relevant questions include:

- Are guests required to show ID?
- Are controls in place to confirm that guests have an appointment with appropriate third-party personnel that day, or are they allowed to walk around freely?

Enterprise assessors may ask to see areas where data are processed. For example, if the third party takes calls from customers on behalf of the enterprise, an assessor should ask to see those areas and observe how the third party manages the staff and the enterprise data there. Assessors should physically follow the data flows laid out in the data flow diagram, tracing the data path throughout the third party.

Many third parties try to limit an assessor's time to just the data center; others (as is often the case with cloud

[15] Cloud Security Alliance, *Consensus Assessments Initiative Questionnaire v3.0.1 (9-1-17 Update)*, https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-0-1/
[16] Santa Fe Group, "Standardized Information Gathering (SIG) questionnaire," https://sharedassessments.org/sig/
[17] *Op cit* NIST, Special Publication 800-53 Revision 4, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[18] International Organization for Standardization (ISO), *Information technology — Security techniques — Code of practice for information security controls*, ISO/IEC 27002:2013, October 2013, https://www.iso.org/standard/54533.html
[19] Freund, Jack; "Using Behavioral Interview Techniques to Assess Supplier Security Posture," The Risk Doctor, 1 October 2014, https://riskdr.com/2014/10/01/using-behavioral-interview-techniques-to-assess-supplier-security-posture/

providers) try to prohibit the assessor from visiting the data center entirely. In the former case, assessors should insist on visiting other locations, or even rotate site visits over time, looking at the data center one time, and the call center another time, etc. In the latter case, if an onsite visit to the data center is prohibited outright, the assessor must decide whether to recommend dropping the third party to business owners, or continue the relationship with a qualified statement in a risk acceptance that the enterprise is unable to conduct onsite validation. Such cloud providers typically point to the sheer number of clients they have and indicate that they simply cannot accommodate that number of onsite visits. Typically, they also provide some alternative documentation to show that they have third-party verification of their controls, so further assessment is unnecessary.

Many third parties try to limit an assessor's time to just the data center; others (as is often the case with cloud providers) try to prohibit the assessor from visiting the data center entirely.

For enterprises that are trying to stretch their third-party risk assessment budget, instead of physically flying staff to various third-party locations, they take advantage of technology, conduct their interviews over videoconference equipment and request virtual walkthroughs via video. Some enterprises hire national firms to conduct their onsite reviews for them, or leverage other enterprise staff in the area to avoid travel charges and limit the impact on assessment personnel.

Technology-aided Reviews

Software vendors can assist with the third-party risk assessment processes in several ways. Many applications facilitate assessments by increasing automation. For example, if an enterprise solicits documents from third parties, or gathers responses to a questionnaire, a software-as-a-service (SaaS) vendor may offer services to:

- Upload documents
- Complete questionnaires
- Score third-party responses
- Notify the enterprise of next steps (such as manual review of uploaded files)
- Schedule an onsite review

Some vendors provide staff to conduct onsite reviews for the enterprise, to augment the capabilities of enterprise staff. Other vendors offer a repository of completed third-party assessments.

For providers with many customers, responding to a bespoke assessment from each can be prohibitively time-consuming. Instead, some third parties opt into a voluntary association where they complete one assessment and make the results available to all organizations that need them. The Cloud Security Alliance® (CSA) offers a version of this service for cloud service providers, called the Security, Trust and Assurance Registry (or STAR Registry).[20] The Santa Fe Group also has a questionnaire framework called the Standardized Information Gathering (SIG) tool, although with no central repository for sharing.[21] Other vendors offer opt-in information sharing repositories, such as the Vendorpedia™ Third-Party Risk Exchange, which houses a collection of independently gathered information about a company and contributed items.[22] It can also include the results of onsite assessments to significantly expedite an assessment process.

Lastly, there are several online repositories of incidents that an enterprise can search to determine whether any relevant events affect a given third party (many third-party software services include these as well). One such free, nonprofit service is the Privacy Rights Clearinghouse, which makes thousands of public data-breach records available for searching.[23] There are also paid services, such as Risk-Based Security Cyber Risk Analytics (formerly the free Datalossdb service)[24] and OneTrust's DataGuidance.[25]

[20] Cloud Security Alliance, "CSA Security Trust Assurance and Risk (STAR)," https://cloudsecurityalliance.org/star/
[21] *Op cit* Santa Fe Group
[22] Vendorpedia, "The World's Only Security and Privacy Third-Party Risk Exchange," OneTrust, www.vendorpedia.org/
[23] Privacy Rights Clearinghouse, "Empowering Consumers. Protecting Privacy.," www.privacyrights.org/
[24] Cyber Risk Analytics, "Actionable Vendor Risk Management," www.cyberriskanalytics.com/
[25] OneTrust, "OneTrust Acquires DataGuidance, Integrates Hundreds of Privacy Laws into OneTrust Privacy Management Technology," 11 March 2019, www.onetrust.com/company/news/press-releases/onetrust-acquires-dataguidance/

Software can also assist in the control-assessment space. In addition to conducting surveys about third-party control posture, various firms enable enterprises to view the results of an automated control evaluation, typically done via scanning tools. These tools gather whatever information they can about a third party from sites on the dark web, and perform the equivalent of an unauthenticated scan against the third party's public-facing systems. The tools look for botnet activity coming from Internet Protocol (IP) addresses associated with the third party. The tools can evaluate the status of secure sockets layer (SSL) certificates. Results are holistically scored on an ordinal scale, and a security rating is extrapolated from the score (in some cases, a security maturity rating may also be assigned).

Various assumptions underlie these approaches and should be called out. While automation can evaluate a large number of third parties expediently, the scope of resulting assessments can be very limited, and may not reflect the use case(s) for which the enterprise employs the third party. For example, if an enterprise allows its SSL certificate to expire on an external system—but that system is not used in the business process and data flows in the contracted work—it might have limited applicability to the enterprise evaluation of that third-party risk posture. It may be indicative of an overall lax approach to security, or it may be the result of a risk-based approach to certificate management. The usefulness of this can vary, so it is important to include a level of analyst discretion in the enterprise assessment model.

Risk Analysis

After all third-party evaluations are complete, the risk analyst puts the results into a risk calculation function. Processes based on standards such as ISO or NIST recommend that enterprises consider assets at risk, threats to those assets and all associated controls; enterprises should then synthesize the data points to produce a holistic risk rating for that third party. This is a high-level version of a risk assessment process that is applicable to any IT asset inclusive of third parties. Because these risk assessment standards tend to be silent on the specifics of how to arrive at a risk rating, it is important to discuss briefly some ways to improve the rigor and reliability of the enterprise third-party risk rating process (or risk analysis process).

Processes based on standards such as ISO or NIST recommend that enterprises consider assets at risk, threats to those assets and all associated controls; enterprises should then synthesize the data points to produce a holistic risk rating for that third party.

The first critical component of conducting a risk analysis is to become clear about what is at risk, and what the results of the third-party assessment actually tell the enterprise about its risk posture. This is where the notion of a fully qualified risk statement becomes important. Fashioned after a fully qualified domain name, this is a complete statement of harm that allows the enterprise, at a glance, to see who is failing, what is failing and the impact. Two examples of such risk statements follow:

- Privileged insiders at a third party use legitimately granted credentials to access customer records and compromise their confidentiality.
- Cybercriminals leverage software vulnerabilities in externally facing systems of a third party, resulting in a service outage of a critical business process.

These statements provide critical information at a glance. First, it is known who is doing or initiating the actions. This is not meant to be a clear statement of attribution; indeed, attribution is very hard and not typically necessary for risk analysis. Instead, it helps an enterprise to be very clear about which threat actor communities are in play. This gives the enterprise a key piece of data around building the first important risk analysis variable: frequency of loss.

With this, the enterprise can estimate how often these threat communities are making a move on a critical asset.

The next data point critical to understanding the overall risk posture is where the failure occurred. This section in particular is informed by the results of the third-party assessment thus far. The results provide insight into third-party control deficiencies. Perhaps during the onsite walkthrough the enterprise assessors noticed that the data center had a false ceiling, so they can see that the physical security controls protecting enterprise data at the third party's location are diminished. Often these control deficiencies need to be aggregated into categories of control deficiencies/failures in order to analyze them at the appropriate level. For example, in the second example risk statement, software vulnerabilities may encapsulate unpatched systems, zero-day vulnerabilities, misconfigurations or installation of remote services tools. Depending on the level of abstraction that the enterprise requires, it can aggregate these control deficiencies together into a high-level category, such as access control failures, endpoint security hygiene or business continuity failures. If more precision is required, the enterprise can also analyze them at more granular levels (this requires a larger number of risk statements to cover all the relevant scenarios).

The last part of the risk statement allows the enterprise to understand fully what the impact to the organization will be. For example, in the first statement, there is a loss of confidentiality (data breach), and, in the second, there is a loss of availability. This is really the most important part of the risk equation, because without the potential for loss, there truly is no risk.

Whatever the findings from the third-party assessment, they are typically expressed in the form of a control deficiency (as part of an overall risk statement). These control deficiencies and failures need to be mapped to a corresponding risk scenario to ensure that the risk associated with these control deficiencies is appropriately rated.

Threat Modeling

Threat modeling is an important part of the risk analysis process. It is important to identify the actors in a loss scenario (not necessarily with the same level of rigor as attribution—though positive attribution can accelerate the process). It is important to understand which third-party controls are successful at defending against the attacks/errors associated with various threat communities. It is important to understand which third-party controls address attacks associated with various threat communities. In some cases, controls may address threats from more than one source; for example, the same control that addresses rogue nation states may also defend against cybercriminals. Overlapping controls in this sense should be noted in the threat model.

Other questions to answer when threat modeling include:

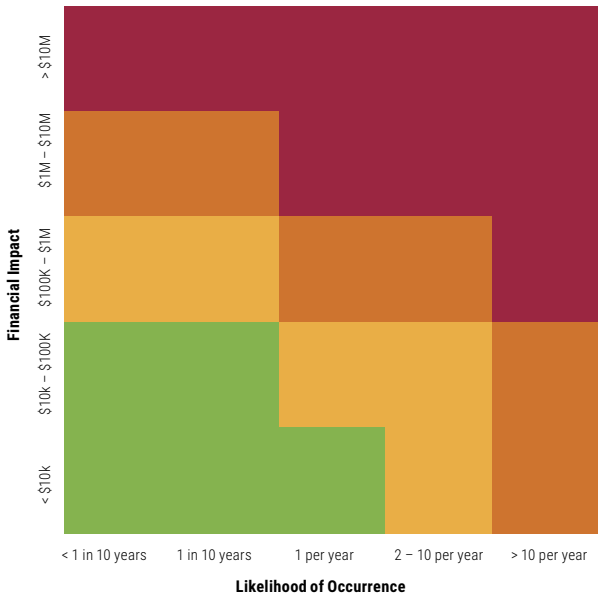
- How often will threat agents encounter enterprise assets at the third-party location?
- What is the danger of discovery posed to that threat agent while it is attempting to compromise those assets?
- What perceived value may enterprise data at the third party hold for an adversary?
- What skills does an adversary need to succeed in compromising third-party systems and accessing enterprise data?
- How much time does an adversary need to compromise systems and access data? What resources and materials does the adversary need?
- What level of effort is required overall from the threat agent to compromise the third party?

The answers to these questions can be collected in a threat profile and maintained for each threat community identified by the enterprise . The profile can be correlated to risk statements, third parties and business processes to gain a clearer picture of end-to-end enterprise risk.

Determining Risk Ratings

A basic approach to risk rating involves the risk matrix, which, in its simplest form, may be expressed in a three-by-three or five-by-five grid. These matrices use two factors—typically probability and impact—to represent the risk that the third party poses to an enterprise. Colors usually signify increasing severity, generally with some reference to an ordinal scale measure (e.g., a 1-to-3 or 1-to-5 scale with no unit of measure, such as time or dollars). Whether it uses verbal labels (low, medium and high), colors or ordinal numbers (such as 1, 2 and 3), the matrix is considered a qualitative representation. **Figure 1** illustrates this with a heat map showing severity as function of likelihood and financial impact. These matrices, although widely used, are typically unable to overcome biases, and do not incorporate validity tests characteristic of more advanced risk analysis methodologies.[26]

FIGURE 1: Third-Party Risk Management Heat Map: Severity as a Function of Likelihood and Financial Impact



Source: Freund, J.; J. Jones; *Measuring and Managing Information Risk: A FAIR Approach*, Butterworth-Heinemann, USA, 2014, https://www.elsevier.com/books/measuring-and-managing-information-risk/freund/978-0-12-420231-3

The ultimate goal of a risk analysis is to deliver a risk rating that drives action in the enterprise. High-risk items should gain the attention of upper management so that they are fully informed of the decisions they need to make. One common mistake is to conduct a risk analysis without first understanding the concerns of management. This lack of understanding often results in a security executive reporting on third-party risk using colors that represent the assessor's view of the risk priority, but the other executives are talking about risk in terms of potential losses to the enterprise.

An advanced approach to third-party risk rating will reflect the economic impact of any third-party data compromise or interruption of service on enterprise business objectives. Fundamentally, the ideal methodology connects cybersecurity consequences to business goals. Understanding the economic impact can also allow enterprises to set aside money to offset potential risk or purchase insurance to help offset financial losses associated with cyberincidents.

Associating risk rating of third parties to potential loss is a highly mature way of understanding the management view of risk and the position of third parties on the risk spectrum. This approach provides the opportunity to assign high, medium and low risk ratings, indexed to potential economic impact, and allows risk management to drive priority through the enterprise and ensure proper remediation of findings.

[26] Hubbard, D.; D. Evans; "Problems with scoring methods and ordinal scales in risk assessment," IBM, *Journal of Research and Development*, vol. 54, no. 3, paper 2, May/June 2010, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.163.4544&rep=rep1&type=pdf

Assessment Closeout and Ongoing Monitoring

After assessment activity concludes, and an overall risk rating is assigned to third parties, certain follow-on activities are required to ensure closure of third-party risk governance processes. These activities vary from enterprise to enterprise, but a rough outline of general practices follows.

Control deficiencies discovered as a part of the assessment are usually documented in a central repository and presented to business owners and others for treatment decisions. Risk owners have the option to accept or mitigate the risk associated with control deficiencies. Risk owners consider the role that compensating controls (if any) can play in the risk response. The organizational role that responds to the control gap often depends on risk ratings; for example, higher risk ratings may merit the attention of upper management.

Control deficiencies discovered as a part of the assessment are usually documented in a central repository and presented to business owners and others for treatment decisions.

Transferring risk is an option, and can be considered a subcategory of acceptance, because remediation of control deficiency is often quite difficult with third parties. For example, many third parties do not make changes unless the contract specifically outlines the control requirements. As a result, remediation of third-party control deficiencies can take several assessment cycles to complete, and often involves more than a single contract cycle. Because the risk associated with the control gap may persist for some time, acquiring insurance may be prudent. This is a critical time for discussion with the business owner to ensure that the control deficiency and how its associated risk impacts the business objectives that the business owner is charged with achieving are understood. Severe control deficiencies can trigger a new contract with a different third party, and enterprise business objectives may incur significant impact as a result.

Many enterprises have some form of third-party governance that presents cyberrisk assessment results alongside other control partner outputs, including country risk and financial risk. This presentation enables an enterprise to gain a holistic view of risk associated with a given third party across multiple domains. A predetermined template may be used to report these results, or each group may have its own report format.

Many enterprises centralize tracking and reporting on risk, including third-party risk, so that all results and work papers are captured in a central location for posterity and auditing reference. Results of prior-year assessments are typically stored in such systems, and can be reviewed when conducting new assessments.

Most enterprises establish a regular cadence for third-party assessment. Often, such cycles are risk based; high-risk third parties may require annual review, while other third parties with less risk are reviewed every few years. The assessment schedule must be documented in the contract with the third party. Statement of frequency must accompany the right-to-audit clause. Some automated third-party management technologies issue notifications when scans or assessments require attention between assessment cycles. For example, if a breach disclosure is detected, the enterprise receives notification, and takes steps to ensure that enterprise data at the third party are properly protected; finally, the enterprise determines whether to initiate the incident response process.

Conclusion

Third-party risk management is a critical component of an overall vendor management program. As more enterprises rely on third parties to help deliver their products and services, third-party risk management will only become more critical over time. Building good enterprise processes, governance and hygiene around third-party management is an important initial step to ensure that third parties are properly vetted before sending data to them. This effort helps to ensure that contracts—including data privacy and security agreements—are executed, and that enterprise data can be presumed reasonably safe under the purview of third parties.

Conducting regular reviews of third-party controls and addressing control gaps and deficiencies ensure that data and service protection is commensurate with the risk that third-party activities pose to the enterprise. Many technologies and software platforms can help to expedite and automate these review processes. Risk ratings are assigned to third parties, criticality to control deficiencies, and gaps are managed through a closeout process that allows an enterprise to properly manage the third party, influence future terms and conditions of the contract, and protect enterprise interests. Managing third-party risk is a critical aspect of cybersecurity programs overall, as the digital walls separating enterprises from third parties are lowered and the world becomes more interconnected.

Acknowledgments

ISACA would like to acknowledge:

Lead Developer

Jack Freund, Ph.D.
CISA, CRISC, CISM, CIPP/US, CIPT, CISSP, FIP
Director, Risk Science, RiskLens, USA

Expert Reviewers

Clemence Chikombingo
CISA
IT Auditor, Midlands State University, Zimbabwe

Dapo Ogunkola
CISA, CRISC, ACA, CFE, CFSA
Internal Audit Manager, Ernst Young, United Kingdom

James C. Samans
CISA, CRISC, CISM, CBCP, CPP, CIPT, CISSP-ISSEP, PMP
Director of Information Systems Security, American Institutes for Research, USA

Scott Solomon
CIPM, CIPP/E
Product Marketing Manager, OneTrust, USA

Board of Directors

Brennan Baybeck, Chair
CISA, CRISC, CISM, CISSP
Oracle Corporation, USA

Rolf von Roessing, Vice-Chair
CISA, CISM, CGEIT, CISSP, FBCI
FORFA Consulting AG, Switzerland

Tracey Dedrick
Former Chief Risk Officer with Hudson City Bancorp, USA

Pam Nigro
CISA, CRISC, CGEIT, CRMA
Health Care Service Corporation, USA

R.V. Raghu
CISA, CRISC
Versatilist Consulting India Pvt. Ltd., India

Gabriela Reynaga
CISA, CRISC, COBIT 5 Foundation, GRCP
Holistics GRC, Mexico

Gregory Touhill
CISM, CISSP
Cyxtera Federal Group, USA

Asaf Weisberg
CISA, CRISC, CISM, CGEIT
introSight Ltd., Israel

Tichaona Zororo
CISA, CRISC, CISM, CGEIT, COBIT 5 Assessor, CIA, CRMA
EGIT | Enterprise Governance of IT (Pty) Ltd, South Africa

Rob Clyde
ISACA Board Chair, 2018-2019
CISM
Clyde Consulting LLC, USA

Chris K. Dimitriadis, Ph.D.
ISACA Board Chair, 2015-2017
CISA, CRISC, CISM
INTRALOT, Greece

Greg Grocholski
ISACA Board Chair, 2012-2013
CISA
Saudi Basic Industries Corporation, USA

David Samuelson
Chief Executive Officer, ISACA, USA

About ISACA

Now in its 50th-anniversary year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Today's world is powered by information and technology, and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISACA leverages the expertise of its 460,000 engaged professionals—including its 140,000 members—in information and cybersecurity, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 220 chapters worldwide and offices in both the United States and China.

About OneTrust

OneTrust® is the #1 most widely used privacy, security and third-party risk technology platform, trusted by more than 3,000 companies to comply with the CCPA, GDPR, ISO 27001 and hundreds of the world's privacy and security laws. OneTrust's three primary offerings include OneTrust Privacy Management Software, OneTrust PreferenceChoice™ consent and preference management software, and OneTrust Vendorpedia™ third-party risk management software and vendor risk exchange. To learn more, visit OneTrust.com or connect on LinkedIn, Twitter and Facebook.

DISCLAIMER

ISACA has designed and created *Managing Third-party Risk: Cyberrisk Practices for Better Enterprise Risk Management* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA®
1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Provide Feedback:

www.isaca.org/managing-third-party-risk

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAHQ

Instagram:
www.instagram.com/isacanews/

DATA SHEET

OneTrust Third-Party Risk Management

HOW THE WORLD MANAGES THIRD-PARTY VENDOR SECURITY AND PRIVACY RISKS

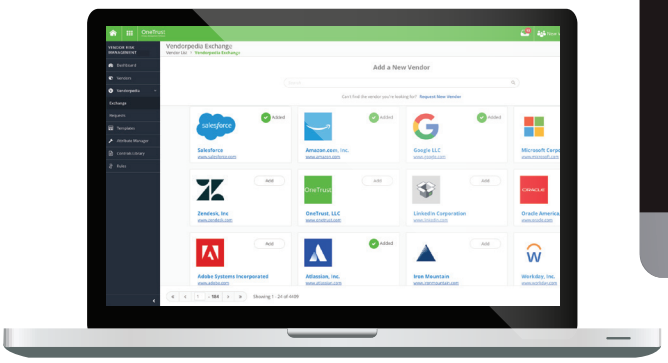
300+
Global Laws Embedded in the Platform

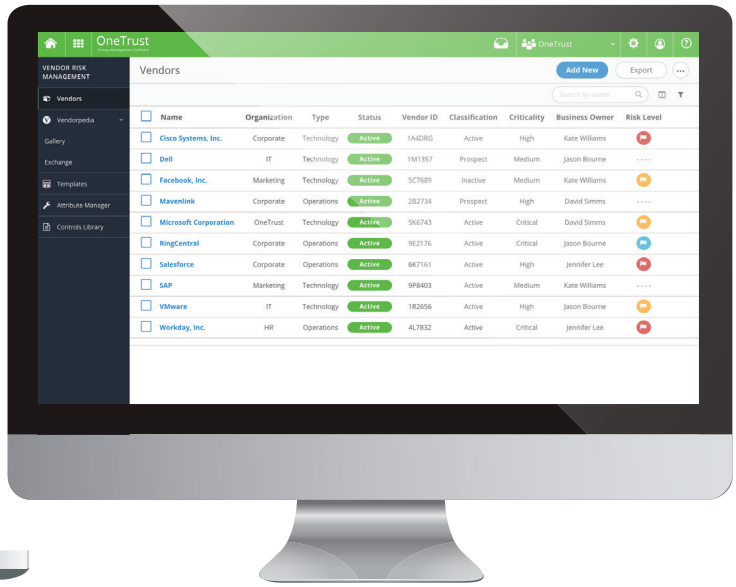
100%
Coverage of the Vendor Risk Management Lifecycle

360°
Third-Party Vendor Visibility

A Centralized Risk Management Platform for Global Security and Privacy Professionals

Third-party vendor risk management isn't a new concept, yet the risks posed to enterprises have evolved. Increasing reliance on third parties, new privacy regulations, shifting cybersecurity threats, and frequent data breaches have upended the third-party risk management landscape. OneTrust Vendor Risk Management is a purpose-built security and privacy solution that directly addresses these challenges and many others.





ASSESS	EXCHANGE	MONITOR
Risk Assessment Automation	**Vendorpedia™ Third-Party Risk Exchange**	**Third-Party Threat Monitoring**
Assess and mitigate third-party vendor risks in less time and with better results	Exchange pre-completed third-party vendor risk assessments and access research on 6,000+ global vendors	Monitor security and privacy threats over time to maintain a watchful eye on third-party vendors

INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2019

OneTrust
PRIVACY, SECURITY & THIRD-PARTY RISK