Whitepaper

Third Party Risk Management Services

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>The risks posed by third-party and fourth-party vendors</td>
<td>2</td>
</tr>
<tr>
<td>An effective third-party risk management process</td>
<td>3</td>
</tr>
<tr>
<td>Phase 1: Categorize third-party intermediaries by level of risk</td>
<td>4</td>
</tr>
<tr>
<td>Phase 2: Background data collection of all third-party intermediaries</td>
<td>6</td>
</tr>
<tr>
<td>Phase 3: Review risk information of all third-party intermediaries</td>
<td>8</td>
</tr>
<tr>
<td>Security questionnaires</td>
<td>9</td>
</tr>
<tr>
<td>Security data categorization</td>
<td>12</td>
</tr>
<tr>
<td>Risk assessments</td>
<td>13</td>
</tr>
<tr>
<td>Remediation</td>
<td>14</td>
</tr>
<tr>
<td>Phase 4: Ongoing monitoring of third-party intermediaries</td>
<td>16</td>
</tr>
<tr>
<td>Attributes of an optimal TPRM process</td>
<td>17</td>
</tr>
<tr>
<td>Third-party risk management services with CyberResearch</td>
<td>18</td>
</tr>
<tr>
<td>Easy of use</td>
<td>18</td>
</tr>
<tr>
<td>Best-in-class third-party risk security</td>
<td>19</td>
</tr>
<tr>
<td>Rapid scalability</td>
<td>20</td>
</tr>
<tr>
<td>Summary</td>
<td>21</td>
</tr>
</tbody>
</table>
Introduction

Vendor due diligence has always been an exemplary response of a vigilant organization. But in light of the SolarWinds supply chain attack, this process has now become less of a best practice and more of an urgent requirement.

Without a comprehensive vendor risk management plan, organizations are completely unaware of any potentially devastating vulnerabilities within their third-party vendor network.

A third-party vendor is any entity that an organization does business with. This includes suppliers, manufacturers, service providers, business partners, affiliates, brokers, distributors, resellers, and agents.

Vendors can be both upstream (suppliers and vendors) and downstream (distributors and resellers), as well as non-contractual entities.

Outsourcing to service providers provides strategic advantages such as cost savings and outside expertise, but also introduces third and fourth party risk.

A fourth-party vendor is a third-party vendor of your third-party vendor.
The risks posed by third-party and fourth-party vendors

Third-party vendors often require access to sensitive information to interact with employees or customers, and integrate with internal systems. This means sensitive data could be accessed by cybercriminals if a third-party vendor falls victim to a cyberattack.

Compromised fourth-party vendors are also a serious threat since they have access to an organization's sensitive data through its third-party vendors.

The concerning vulnerability that results from an inexorable third-party network, has resulted in governments globally enforcing strict vendor risk management regulatory requirements.

Financial institutions and healthcare organizations are under particular regulatory scrutiny, but the practice of third-party risk management is not only limited to these industries. A sagacious organization, within any industry, actively protects its sensitive data from third-party breaches.
An effective third-party risk management process

Third-party risk management (TPRM) is still a novel practice and, as a result, many organizations are unaware of its effective implementation. The four-phase process below presents a highly effective TPRM framework for monitoring all third-party intermediaries and mitigating third-party breaches.

**Phase 1** Categorize third-party intermediaries by level of risk.

**Phase 2** Background data collection of high risk third-party intermediaries.

**Phase 3** Review risk information of high risk third-party intermediaries.

**Phase 4** Ongoing monitoring of all third-party intermediaries.

UpGuard CyberResearch manages this entire end-to-end process on behalf of an organization. CyberResearch incorporates Third-Party Risk Management Services, which includes a comprehensive vendor risk assessment report produced by a dedicated team of professional third-party risk analysts outlining key findings, and facilitation of remediation efforts.
Phase 1

Categorize third-party intermediaries by level of risk

The reliability of a third-party risk management (TPRM) process is proportional to its threat response time. A precipitous disruption to threat progression significantly decreases the chances of third-party breaches and supply chain attacks.

But global rapidity is not the attribute of a superior TPRM process, but rather, its efficient distribution. High risk vulnerabilities need to be identified and remediated first, before lower risk threats.

An optimum threat response distribution concentrates remediation efforts on the most vulnerable sectors of an ecosystem, resulting in the highest recovery of an organization’s security posture.

Quantifying each vendor’s cybersecurity risk status involves a rigorous assessment of multiple attack vectors, a highly-complex process best outsourced to a trusted cybersecurity solution to ensure accuracy.

The final evaluation, represented by a security score, expedites third-party risk categorization, surfacing all vulnerabilities requiring urgent attention.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>801-950</td>
<td>601-800</td>
<td>401-600</td>
<td>201-400</td>
<td>0-200</td>
</tr>
</tbody>
</table>
UpGuard's trusted security rating system is based on an analysis of 70+ vectors:

- Susceptibility to man-in-the-middle attacks
- Insecure SSL/TLS certificates
- SPF, DKIM and DMARC settings
- HTTP Strict Transport Security (HSTS)
- Email spoofing and phishing risk
- Vulnerabilities
- Unnecessary open administration, database, app, email and file sharing ports
- Malware susceptibility
- Network security
- Exposure to known data breaches and data leaks
- Vulnerable software
- HTTP accessibility
- Secure cookie configuration
- Results of intelligent security questionnaires
- 50+ more...
Phase 2

Background data collection of all third-party intermediaries

With all high-risk vendors prioritized, the aggregation of relevant third-party intermediary (TPI) assessment data can commence. The fluidity of this process depends on the location of the data and how readily it can be extracted.

An effective TPRM process is characterised by efficient threat-response distribution. High-risk vulnerabilities need to be identified and remediated first, before lower risk threats.

Third-parties could include:

- Consultants (regulatory and promotional)
- Suppliers
- Distributors
- Event planners
- Brokers
- Resellers
- Logistics intermediaries
- Sales agents
- Partners

By focusing on the most vulnerable attack vectors of an ecosystem, an organization has the highest chances of protecting its security posture and preventing data breaches.

Security issues can occur at any phase of the vendor lifecycle including after the vendor relationship has ended.
For a third-party risk management process to be efficient, an accurate log of all vendors should be maintained. This record won’t only help keep track of all vendor assessments, but it will also aid in the monitoring of each vendor’s security posture.

Some organizations maintain a spreadsheet record of all vendors and their risk assessments, but such manual processes are inefficient and definitely not scalable. An amicable alternative is to keep a digital inventory of all past and present vendors, as offered by the Vendor Risk platform by UpGuard.

Not all TPI data is valid, but only the segments that are relevant to the particular risk assessment that will be undertaken. This filtration process depends upon the specific TPI risk framework being implemented.

Manual TPI data filtration is alleviated on the UpGuard platform with the support of an ever-growing library of third-party risk standards, frameworks and regulations across all industries.
Phase 3

Review risk information of all third-party intermediaries

Many vendors publish details of their security efforts online to facilitate prompt third-party security assessments. To keep third-party risk communications efficient, all published security information should be discovered and aggregated prior to submitting any security questionnaires.

Published security information could include a SOC2 report, ISO 27001 certification, or any other standardized audit reports the vendor makes available.

Though published security information slightly simplifies the third-party risk assessment process, searching for this information is a time-consuming process, especially with a comprehensive vendor network.

This mechanism of data review and categorization can be completely performed by UpGuard third-party risk analysts who are experts in collecting and processing relevant assessment data on your behalf.

If security information is not readily accessible online, a vendor's business sponsor network could be a helpful resource. Otherwise, highly-targeted security questionnaires should be sent to fill all remaining risk data gaps.
Security questionnaires

Security questionnaires (also known as a third-party risk assessment questionnaires) are designed to help organizations identify potential weaknesses among their third-party vendors that could result in a data breach, data leak or any other type of cyber attack.

UpGuard Vendor Risk offers an intelligent questionnaire management solution optimized for expeditious execution.

Standard best practice is to use an industry standard questionnaire as a starting point and then adapting it to an organization's needs. This will keep communication streams efficient, preventing laborious follow up questions to investigate the specific security details of each vendor.

A combination of the following five security assessments present a basis of a robust third-party security questionnaire.

1. **CIS Critical Security Controls (CIS First 5 / CIS Top 20)**

The Center for Internet Security (CIS) is a non-profit entity dedicated to safeguarding private and public organizations against cyber threats. CIS’s 20 controls are a prioritized set of actions to protect critical systems and data from common cyber attacks. These are high-priority, highly effective controls that reduce cybersecurity risk and map to most major frameworks such as the NIST Cybersecurity Framework, NIST 800-53, ISO 27000 series and regulations like PCI DSS, HIPAA, NERC CIP and FISMA.
2. Consensus Assessments Initiative Questionnaire (CAIQ)

CAIQ comes from the Cloud Security Alliance (CSA), an organization dedicated to defining and raising awareness of best practices for secure cloud computing. The questionnaire provides industry-accepted ways to document security controls in IaaS, PaaS and SaaS offerings. These questions are ideal for assessing the risk of third-party cloud solutions.

3. NIST 800-171

The National Institute of Standards and Technology (NIST) offers a north-star metric for data privacy for the U.S. through best practices and standards. The purpose of NIST 800-171 is to help protect controlled unclassified information (CUI) in nonfederal systems and organizations. It contains 14 specific security objectives with a variety of controls and maps to NIST 800-53 and ISO 27001. If an organization offers products, solutions or services to the Department of Defense (DoD), General Services Administration (GSA) or National Aeronautics and Space Administration (NASA) it must comply with NIST 800-171.

NIST CSF

1. Security and Privacy Programs Assessment

1.1. Security and Privacy

Why this section matters: An information security and privacy program is a comprehensive set of policies, guidelines, and processes for identifying and addressing the threats and risks to company information and systems. An established security and privacy program can help assure customers that their information will be safe while it’s in your custody.

1.1.1. Does your company have a strong, established security program, and does the scope of the program include all information processed within the organization?

- [ ] Yes, our security program covers all aspects of information security within the organization.
4. Standardized Information Gathering Questionnaire (SIG / SIG-Lite)

SIG and SIG-Lite were created by the Shared Assessments Program, a trusted source for third-party risk management resources including tools and best practices to manage vendor risk. The SIG questionnaire is a tool to assess cybersecurity, IT, privacy, data security and business resiliency. SIG-Lite is a compilation of higher level questions from SIG and is generally used for low risk vendors.

5. VSA Questionnaire (VSAQ)

The Vendor Security Alliance (VSA) is a coalition of companies committed to improving Internet security. VSAQ was first published in 2016 and is designed specifically to help companies monitor their supplier's security practices. It contains six sections: data protection, security policy, preventative and reactive security measures, supply chain management and compliance.

Thousands of potential questions could be extracted from these frameworks and adapted to suit an organization's needs and priorities.
Security data categorization

To simplify information digestion, vendor security data should be grouped into relevant categories. The categories depend on the level of risk associated with each vendor.

Some suggested categories are as follows:

- Period of business relationship
- Data bank location
- Country of service operation
- Industry type
- Level of government involvement
- Relationship type
- Volume of data transactions
Risk assessments

Vendor security assessment questionnaires are just a single dimension of a multi-dimensional practice of verifying the security of third-party vendors.

For a more accurate presentation of a Vendor's security posture, questionnaires should be used in harmony with security ratings.

Security ratings fill the large gap left from traditional risk assessment techniques like the SIG questionnaire or VSA questionnaire. They complement and provide assurance of the results reported in security questionnaires because they are externally verifiable, always up-to-date, and provided by an independent organization.

The UpGuard platform continuously scans vendor networks and rates the security posture of each third-party with a best-in-class security scoring system.

UpGuard CyberResearch empowers organizations to completely outsource third-party risk assessment of all vendors to cybersecurity analysts. The details of each risk assessment is collated in a comprehensive report to keep organizations informed of all present risks lurking in their third-party network.

To further elevate the standard of vendor due diligence, UpGuard CyberResearch also offers Vendor Data Leaks assessments.

This additional layer of analysis empowers organizations to predict which of their vendors are likely to experience a data breach, facilitating preemptive action to significantly dampen the effects of third-party breaches.
Remediation

An organization's resilience to third-party breaches isn't only measured by its detection capabilities, but also its remediative action. Prompt remediation in line with a clear incident response plan is critical.

There are two incident response frameworks that have become industry standard, the NIST Incident Response Process and the SANS Incident Response Process.

The NIST Incident Response Process is as follows:

1. Preparation
2. Detection and analysis
3. Containment, eradication and recovery
4. Post-incident activity

Whereas, the SANS Incident Response Process is as follows:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons learned

A majority of the NIST and SANS frameworks overlap, the primary differentiators are verbiage and process clustering.
Regardless of the specific framework, every Incident Response plan should:

- Provide an overview
- Identify and describe roles and responsibilities
- Be tailored to specific business risks and needs
- Outline the current state of information security, data security and network security
- Have clear detection and identification procedures
- Specify tools, technologies and resources needed for containment and eradication
- Outline recovery and follow-up tasks
- Have a communication plan
- Be well tested
- Have version control or a section to outline when and who made revisions

UpGuard CyberResearch manages the entire remediation process for all identified threats, relieving the pressure of instituting and managing an in-house Incident Response plan.
Phase 4

Ongoing monitoring of third-party intermediaries

For the highest protection against third-party breaches, organizations need to continuously cycle between monitoring and assessing all third-party vendors. The risk of a data breach is ever-present, even after a prospective vendor passes an initial assessment.

Without visibility into the most up-to-date security posture of all vendors, it is not possible to identify and remediate newly surfaced vulnerabilities.

UpGuard Vendor Risk instantly alerts organizations when a particular vendor’s security score drops, prompting the instant submission of industry and regulatory specific questionnaires.

An intelligent vendor security scoring systems, gives stakeholders instant visibility into the health status of their entire vendor network for an accurate representation of the likelihood of a third-party or supply chain breach.
Attributes of an optimal TPRM process

- An end-to-end third-party risk workflow with real-time vendor risk monitoring and tracking of remediation progress across various assigned roles.
- A comprehensive digital repository of past and present vendors and their history of risk assessments.
- Global third-party risk remediation visibility through scoping executive reporting.
- Facilitates third-party risk assessments with best-in-class vendor security regulatory standards.

- Minimal learning curve for rapid implementation and vendor risk assessment execution.
- Provides the capability of completely outsourcing vendor monitoring, risk assessments and remediation to world-class third-party risk analysts.
- A cost-efficient and rapidly scalable solution to support unimpeded third-party breach protection for growing businesses.
Third-party risk management services with CyberResearch

CyberResearch by UpGuard empowers organizations to scale their third-party risk management program cost-effectively, by combining a dedicated team of third-party risk analysts and an easy-to-use SaaS platform.

Unlike traditional managed services which typically bundle a thin layer of poorly-integrated software with expensive consultants, CyberResearch is both intuitive and easy to use. With a click of a button, you can request a risk assessment, chase a vendor for evidence, or get help with remediation of identified risks.

CyberResearch has been intentionally engineered to meet the optimal TPRM process across all industries.

Ease of use

CyberResearch was developed to support the essential requirements of end-users, with a chief focus on rapid implementation and execution. With the perpetual support of a dedicated third-party risk analyst team, organizations can instantly assume a firm grasp of their third-party risk mitigation efforts.

- Instantly request vendor assessments directly from the platform and a dedicated risk analyst will complete the end-to-end process on your behalf.
- Monitor the security posture of all vendors to identify any third-parties at risk of a data breach.
- See the status of each vendor’s assessment with real time updates to streamline the logistics of risk assessments.
- View third-party risk remediation protocols to track the progress of vendor security posture straightening efforts.
Best-in-class third-party risk security

Entrust risk assessments to a world-class third-party risk analyst team committed to cultivating the sharpest techniques for monitoring and assessing third-party risks.

With the support of analysts, organizations can outsource the pressure of conducting and managing risk assessments.

- **Remain informed of the findings of each risk assessment through comprehensive reports created by risk analysts.**
- **Implement the most astute third-party risk due diligence with risk assessments that meet the highest of regulatory standards.**
- **Improve the consistency and accuracy of all risk assessments by entrusting the entire process to third-party risk experts.**

---

Vendor portfolio risks

<table>
<thead>
<tr>
<th>Finding</th>
<th>Risk</th>
<th>Category</th>
<th>Vendors at risk</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>MySQL</code> port open</td>
<td>Critical</td>
<td>Network Security</td>
<td>20 / 400 vendors</td>
</tr>
</tbody>
</table>

The 'MySQL' service is exposed to the Internet. Server configuration should be reviewed and ports closed.

- **PiperChat** (`piperchat.com`)
  - 721 domains
  - Request remediation

- **Hooli** (`hooli.com`)
  - 524 domains
  - Request remediation
Rapid scalability

CyberResearch provides the most cost-effective solution for rapidly scaling an organization’s third-party risk due diligence efforts. The support of a dedicated risk analyst team removes the costly requirement of establishing an internal team of third-party risk experts.

- Instantly increase or decrease the number of vendors that require assessment without having to adjust an internal third-party risk assessment team accordingly.
- Avoid the logistical struggles of managing risk assessment for a comprehensive vendor network.
- Rapidly scale vendor assessment efforts in line with growing business requirements.

### Managed vendors

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Status</th>
<th>Score</th>
<th>Last assessed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pied Piper</td>
<td>In progress</td>
<td>721</td>
<td>Dec 18, 2020</td>
</tr>
<tr>
<td>piedpiper.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hooli</td>
<td>Completed</td>
<td>580</td>
<td>Dec 18, 2020</td>
</tr>
<tr>
<td>hooli.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PiperChat</td>
<td>Completed</td>
<td>324</td>
<td>Dec 18, 2020</td>
</tr>
<tr>
<td>piperchat.com</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
In summary

- US government data breach highlights the global necessity for a diligent third-party risk management process.
- Organizations struggle to keep up with the evolving regulatory pressures of third-party risk management.
- The challenge of a successful TPRM program is to combine ease of implementation and rapid scalability with the most rigorous third-party risk security practices.
- Deep visibility into the security posture of an entire vendor network is the key to instantly identifying and, therefore, mitigating third-party risks.
- By outsourcing the entire third-party risk assessment process to expert analysts, organizations can relieve the pressure of manually managing assessment processes and ensuring adherence to strict regulatory standards.
Questions? We have answers
We're here to help, shoot us an email at sales@upguard.com

Know your vendors. Secure yourself.
Looking for a better, smarter way to protect your data and prevent breaches?
UpGuard offers a full suite of products for security, risk and vendor management teams.

Contact sales  Free demo →

Trusted by hundreds of companies worldwide

www.upguard.com  650 Castro Street, Suite 120-387, Mountain View CA 94041 United States
+1 888-882-3223

© 2021 UpGuard, Inc. All rights reserved. UpGuard and the UpGuard logo are registered trademarks of UpGuard, Inc. All other products or services mentioned herein are trademarks of their respective companies. Information subject to change without notice.