Optimizing Third Party Cyber Risk in the Enterprise
Who is This For?
This handbook is designed for IT professionals and management who want to understand third party cyber risk and how it can be optimized in the enterprise. Third party cloud leaks have a massive impact on an organization; this handbook is for those interested in what can be done proactively to prevent them. Some technical understanding is expected for the procedural details of cyber risk assessment and mitigation. For a business perspective on vendor risk, see our handbook The Executive Guide to Third Party Cyber Risk.

What Will be Covered?
We will define cyber risk, understand why third party risk is especially important, and look at some real world examples where vendor cloud leaks have had major consequences for all involved. Then we will look at how cyber risk can be measured, what threat protection and hardening can be observed from an outside perspective, and how risk scoring allows organizations to manage a network of vendors at scale. Finally, we will look at creating third party acceptance criteria so that information and technology vendors can be vetted to reduce the overall risk of data outsourcing.

About This Handbook

What is UpGuard?
UpGuard is the world’s first cyber resilience platform, designed to proactively assess and optimize business risks posed by information technology. We help businesses automate and validate their IT processes to create resilient assets. We’ll include some examples of how we do this later in the handbook.
What is Cyber Risk?

Put simply, cyber risk is the potential damage that can be done to an organization through its information and technology. Data breaches, cloud leaks, and major outages impact companies both financially and reputationally. Despite increased spending on cybersecurity solutions, businesses have been unable to reduce their frequency or impact. This is because most cyber risk is caused by operational error, not sophisticated external attacks. The most common vector of breach and outage is misconfiguration: a server left with a default account and password; a database with a blank password; a cloud storage instance left open to the internet, an SMB port accidentally left open to a Windows server— the list could go on forever.

The complexity of modern enterprise data centers necessarily entails more configuration than humans are able to efficiently process. Accidents, oversights, and even negligence leave enterprise IT systems in a fragile state, with corporate data often exposed as a result. At scale, standard processes such as server deployment or application migration require special care to ensure that resilient assets are deployed in production— and to optimize the cyber risk faced by the business.
Third Party Problems
But modern enterprise data centers extend beyond the boundaries of a physical server room, beyond even the cloud, and reach into vendors, partners, and any other third party with access to the company’s information or computing systems. Every copy of a production data set is a vector for breach; handing those data sets to a third party also hands them the attendant risks, with the implicit trust that they will take necessary steps to mitigate that risk and protect the data. Unfortunately, this assumption is faulty. Like any company, information vendors such as analytics processing or statistical analyses firms utilize digital infrastructure, email, websites, cloud services, and as such, face the same challenge to streamline and harden operational processes. When a vendor places a customer data set into the cloud and accidentally leaves it open to the internet, it’s the primary company who takes the brunt of the blame. It’s their data, and their customers will not be moved by the fact that the leak occurred with a vendor. The trust relationship damaged in a cyber incident exists between a customer and a brand—the internal (and outsourced) technical workings of the brand do not factor into the public’s response to a breach.

Real World Examples
Many of the largest and most well known breaches are cases of third party information exposure.

RNC Vendor Data Root Analytics Exposes 198 Million Voter Records
One of the largest leaks of all time was discovered when an exposed cloud system was found, containing both collected and modeled voter data from Data Root Analytics, a firm contracted by the RNC for data driven political strategy. Over 198 million unique individuals were represented in the data set, with personal details, voter information, and modeled attributes including probable race and religion.

Government Contractor Booz Allen Hamilton Leaves Geospatial Data and Credentials Exposed
Another exposed cloud storage instance revealed data from government contractor Booz Allen Hamilton. In addition to data exposure, the bucket also contained encryption keys for a BAH engineer and “credentials granting administrative access to at least one data center’s operating system.” In this case, not only was information compromised, but further systems could have been as well, allowing malicious actors to hop from a publicly exposed cloud server to an authorized server on the network.

Scottrade Bank has 20,000 Customer Records Exposed by Third Party Genpact
Information vendor Genpact was ultimately responsible for exposing sensitive loan application data from Scottrade Bank for over 20,000 unique individuals. Yet again, the vendor had stored the primary company’s data in the cloud without the proper protection.
Measuring Third Party Cyber Risk

External Assessments
Without thoroughly examining the internal digital infrastructure of a company, it's impossible to get a complete picture of their cyber risk; however, there are many things that can be learned through an external examination that reflect on overall posture and telegraph internal practices in such a way to give an idea how risky a particular vendor is. In this section we will look at what these external factors are, what they tell us about an organization, and how they can be used to measure third party risk at scale. We'll also look at their limitations and see how external assessments can be supplemented to answer critical questions about a vendor's data handling practices.

How UpGuard Helps
UpGuard's Cyber Risk product helps businesses navigate their vendor relationships by providing automated external assessment and risk scoring. Simply add your vendors and UpGuard does the rest.

Microsoft

External Cyber Risk Score

689 / 950

$85B VALUATION  131,287 EMPLOYEES  Redmond, WA  Satya Nadella, CEO  95% Approval Rating

Websites (8,000)
Phishing and Email
Phishing is a method of cyber attack that attempts to trick a person into giving up their password or some other sensitive data to an unauthorized third party. Spearphishing is when these attempts are laser-focused, with target specific customization and messaging, increasing the likelihood of success. For an information vendor, a successful phishing attempt could secure the keys to terabytes of customer data, so it is critical that they be protected against these kinds of attacks.

SPF, DKIM, DMARC
The most efficient way to beat phishing attacks is to ensure they never reach a real person. Spam filters and email servers, when properly configured, can drastically reduce the quantity of phishing emails that land in a person’s inbox. They do this by validating and authenticating the email against various sources to ensure it is from who and where it says it’s from. The three most common methods of doing this are the Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC).

- SPF - Verifies that the email originated from a server trusted by the sender’s domain.
- DKIM - Verifies that the email originated from the sender’s organization.
- DMARC - Specifies how to handle SPF and DKIM validated email.

All of these mechanisms rely on DNS to function, which means that a public DNS record must exist to give mail servers and spam filters the necessary information for them to work. In terms of vendor assessment, this means third parties can be independently verified to have protection against email phishing attacks. Companies who lack these free and relatively easy to implement protections are far more likely to be hit with a successful phishing attempt.

How UpGuard Helps
UpGuard validates that vendors are employing phishing protection for their domain.

<table>
<thead>
<tr>
<th>SPF Enabled</th>
<th>SPF records prevent spammers from sending messages with forged addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS &gt; SPF exists</td>
<td></td>
</tr>
<tr>
<td>EXPECTED</td>
<td>true</td>
</tr>
<tr>
<td>ACTUAL</td>
<td>true</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DMARC Enabled</th>
<th>DMARC protects against fraudulent emails being sent from your domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS &gt; DMARC exists</td>
<td></td>
</tr>
<tr>
<td>EXPECTED</td>
<td>true</td>
</tr>
<tr>
<td>ACTUAL</td>
<td>false</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNSSec Enabled</th>
<th></th>
</tr>
</thead>
</table>
Website Encryption and Software
A company’s website is often their primary customer interface. It’s also a telling representation of their overall risk posture. Unencrypted websites, or those without the proper SSL configuration, can leak customer data by transmitting it in plain text over the internet or having it intercepted by a man-in-the-middle. Furthermore, web servers running vulnerable software or code are indicative of ineffective hardening and maintenance processes. The following attributes can be independently measured for a vendor’s website:

- **SSL Encryption Details** - This includes whether SSL is enabled, enforced, and sitewide. It also covers certificate details like cipher suite, encryption strength, and expiration date.
- **Software Type and Version** - Without proper obfuscation, an anonymous person on the internet can learn what software is running on a website, including what version. This focuses the avenue of attack and allows known vulnerabilities in the revealed software to be probed for exploitation. Scripts running on the website can also reveal vulnerabilities.

Each of these factors is an example of resilience. As the collection of external factors grows, a better picture is painted of how each vendor handles cyber risk management within their own systems—a good measuring stick for how they will handle your data.

**How UpGuard Helps**
UpGuard finds domains and websites associated with your vendors and performs a thorough external assessment of them.

---

### WEBSITE

<table>
<thead>
<tr>
<th>Website</th>
<th>397/950</th>
<th>5/8</th>
<th>Fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Enabled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL</td>
<td>exists</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Suspected Phishing Page</td>
<td>Pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suspected Malware Provider</td>
<td>Pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suspected Unwanted Software</td>
<td>Pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X-Powered-By-Header</td>
<td>Fail</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Companies who lack these protections are far more likely to be hit with a successful phishing attempt.
Open Ports
The principle of least privilege would have as few ports as possible open to the internet, in order to minimize the potential attack surface. For a web server, ports 80 and 443 would be typical. When extraneous ports are left open, numerous risks arise, including attacks such as the WannaCry and Petya ransomware strains which exploited open Microsoft SMB ports (135-139, 445) using the EternalBlue mechanism.

Some examples of dangerous open ports include:

- **Telnet (23)** - An open telnet port usually means an active telnet server. Telnet is extremely insecure and should never be used in the enterprise.

- **FTP (21)** - FTP is an unencrypted file transfer protocol, meaning that information passed through it is susceptible to third party intrusion. SFTP and many other options exist to replace it.

- **MSSQL (1433, 1434)** - Databases should never be exposed to the internet directly. All database manipulation should happen through carefully controlled front-ends. Direct database access from outside the network should require a VPN connection.

- **MySQL (3306)** - Exposed databases can be misconfigured to allow anonymous access to any and all data contained within. Whether Linux or Windows, these database ports should be disallowed to the internet.

- **SSH (22)** - SSH is an encrypted protocol and there are times when it is appropriate to face the internet, but for the most part it should be limited to gateway servers from which an authenticated user can hop to another system inside the network. Exposing remote administration ports to the internet can lead to system compromise in the event of a weak, blank or default password, botched permission set, or vulnerability in the software.

- **LDAP/AD (389)** - Directory information should always be passed over an encrypted connection (636 in this case), but often directory information should not be exposed to the internet at all. Without careful consideration, this can lead to a massive leak of corporate structure, user account names, and other directory information.

For vendor risk assessment, if extra or dangerous ports are open, at the very least the IT team can ask the vendor why, and better understand their data security practices. Without empirical evidence, teams are often left to take vendors at their word, which is a poor way to measure the business risk of a possible new partnership involving the transfer of business critical customer information across the internet.

**How UpGuard Helps**
UpGuard scans every discovered vendor domain for open ports and tracks the results over time.
Other Information
A few other things can be independently verified:

- **Domain Expiration** - Domain name maintenance is a basic function of maintaining a digital presence. An expiring domain reveals an alarming broken process.

- **Blacklisting** - When a domain exhibits an exceptional amount of suspicious activity (usually because their systems were compromised by a third party) it is added to blacklists so that other organizations can preemptively block communications originating from it. A blacklisted vendor raises an immediate red flag.

- **DNS Configurations** - DNS poisoning/spoofing is one way attackers direct traffic to malicious systems. Implementing security measures like DNSSEC helps to protect against such attacks and verify DNS requests so that when someone types in a URL it always goes to the right server.

How's Business?
Finally, there is some general information about the vendor that should be considered alongside the more technical assessment. The risk a vendor brings when handling your data increases if their culture or environment is not healthy. By understanding employee satisfaction and leadership approval rating, another aspect of the business can be understood before entrusting them with your data.

How UpGuard Helps
UpGuard checks vendor domains for expiration and blacklisting and validates secure DNS configurations. Further, we incorporate business data from Glassdoor to analyze company health.
When teams lack empirical evidence, they are left to take vendors at their word.
Risk Scoring and Continuous Assessment

None of these factors by themselves tell much of a story, but aggregated together, they do begin to illustrate how an organization mitigates cyber risk for themselves and their customers. By quantifying this data into a risk score, vendors can be easily compared to one another in a way that allows you to make better decisions when choosing a company to employ. Technical team members can understand the detailed risks each vendor poses, while management can work from a higher vantage that focuses on overall risk exposure.

Third parties are cyber risk vectors for as long as they have your data. Assessments should continue throughout the vendor relationship to ensure that your expectations of risk aren’t misplaced due to a change that was made after the initial assessment. This way, teams can have up to date information about vendors and proactively make choices to optimize risk.

How UpGuard Helps

UpGuard aggregates all discovered external risk factors into a single score. This score represents the total cyber risk a vendor presents. Because UpGuard regularly assesses vendors, this score always reflects the current risk status.

Establishing Vendor Acceptance Criteria

Acceptable Risk

As with any type of risk, third party cyber risk can only be optimized, not eliminated. The goal is to understand and minimize risks so the business has the best chance of succeeding. As such, cyber risk assessment should factor into how information technology vendors are chosen and measured. Establishing a set of operational criteria that a vendor must meet in order to handle your data helps reduce the amount of risk you take on through third parties. These can be simple criteria, such as maintaining an acceptable risk score, or more thorough criteria, with technical specifics outlined in detail. We'll look at a few of the ways this can be accomplished, along with other questions to ask a vendor before entrusting your data to them.

Thresholds

With a standardized risk scoring method, vendors can be held to the same objective criteria across the board. This allows companies to designate an acceptable level of risk when choosing vendors and create policies that are effective at scale.

Risk Scoring With UpGuard

UpGuard quantifies and visualizes vendor risk by automating external technical assessment and translating it into business terms.
As long as third parties have your data, they are cyber risk vectors.
**Threat Protection**

Additionally, you can require that a vendor meet certain technical criteria in order to handle your data. More than some arbitrary requirement, these criteria can be the difference between an attack succeeding and failing. For example:

- **Email Protection** - Require that vendors have protection against phishing scams in place.
- **Website Encryption** - Require vendors to use SSL and encryption best practices.
- **Port Management** - Require vendors to not have specific ports open, especially those for databases and file transfers.

Depending on your business and the type of data you’re outsourcing, you may want to specify certain protections that apply.

**Business Risk, Technical Detail**

In addition to the risk score, UpGuard includes the technical assessment details for every vendor, so that IT teams can know specifically what questions to ask and what threats pose the greatest risk.

**Vendor Questionnaire**

In addition to the external technical assessment, it’s also important to ask your vendors about their data handling practices and procedures. Having a standard questionnaire for vendors to fill out can help streamline the discovery of red flags. Here are some example questions to include:

- Do you store data in the cloud? If so, what steps do you take to protect that data?
- How many copies of the data will the vendor keep? Will all of them be secured?
- Will copies of the data be stored on laptops or other workstations and mobile devices?
- Will the data ever be transmitted over an unencrypted connection?
- How is access to customer data segregated for employees of the vendor?

This is just a beginning, but the most important takeaway is that outsourcing analytics processing or other information work to a third party requires careful consideration of how they will secure that data. Establishing a policy and a process to govern vendor assessment can drastically reduce the amount of total cyber risk for any business.
Conclusion

The information economy is here to stay, and outsourcing data analysis to specialized vendors is a key part of it. But like any business partnership, the risks should be understood and optimized before moving forward. Since these are vendors dealing with information and technology as their business, they should be assessed from an IT perspective. Establishing thresholds of acceptable risk helps class vendors and differentiate them using a standard that matters. Consider all the measures you take to secure your own data and infrastructure. Holding your vendors to similar standards continues that protection throughout the data's chain of custody, because it's only as safe as the weakest link in that chain.
UpGuard is the world’s first cyber resilience platform, designed to proactively assess and manage the business risks posed by information technology. By validating and automating IT processes, we help organizations build resilient digital businesses on-site and in the cloud.