The Executive Guide to Third Party Cyber Risk
About This Handbook

Who is this for?
This handbook is intended for executives and business leaders who wish to understand cyber risk, specifically the cyber risk taken on by outsourcing data handling to a third party. Although some technical information will be alluded to, this handbook presents cyber risk from a business perspective.

What will be covered?
We will define cyber risk and cyber resilience, and show why they matter for businesses. We’ll examine the information economy and how it affects the trust between customers and businesses, and look at some real world cases where that trust was damaged. The core of the handbook will detail how to build a resilient digital ecosystem of vendors, how to assess their security practices, and ultimately how to understand what kind of risk is taken on by giving them business data. Finally, we will touch on cyber insurance and how third party risk fits in.

What is UpGuard?
UpGuard is the world’s first cyber resilience platform. We help companies assess and mitigate the business risks posed by technology by validating and automating IT processes. We’ll show some examples of how UpGuard does this later in the handbook.
Introduction

What is Cyber Risk?
Put simply, cyber risk is the set of threats a business takes on when they employ technology and utilize information. These risks are often overshadowed by the immense value information technology provides, allowing businesses to move faster, communicate to wider audiences, improve processes with data, and digitize and automate burdensome manual and physical workflows. But information technology also opens a new vector of business risk, where not just the technology, but the business itself can be compromised if it is not accounted for.

From email scams that trick people into giving out their password or making unauthorized financial transactions, to ransomware that locks out critical assets, to unexpected outages that halt operations, to multimillion record data breaches that expose customer data to the world—by now most businesses are familiar with cyber risk, even if they don’t yet think of it in those terms. There can be no doubt that business has reaped massive rewards from the value information and technology offer, but the question determining success going forward will be: who can mitigate their risks?

A Business Problem.
As technology gained a foothold in business and began to expand, technological concerns were often relegated to the IT department, with the expectation that they should just “make it work.” But information and technology are no longer ancillary parts of the business, no longer cost centers or maintenance departments. Technology is now so thoroughly integrated with business operations that it has become a core pillar of every contemporary organization.

As such, the risks posed by that portion of the business are no longer limited to IT either. Breaches and outages are business problems first and technical problems second. Consider the following in the wake of a major cyber incident:

- Customer and public reaction
- Legal action taken
- Ongoing reputational damage

In all three cases, the damage resulting from a cyber incident affects the company as a whole, not just the piece responsible for the error. Because the brand is held responsible, representatives of the brand, executives and the board, must bear the brunt of the public outcry, and face professional and even personal repercussions for the mishandling of customer trust. Ongoing reputational damage leaves a stain on a company’s history, even after firing a sacrificial exec and instituting costly new security measures. The real kicker is that this is true even if the incident occurred with a vendor.

Ironically, executives rarely have visibility into the IT operations, in-house and outsourced, that lead to breaches and outages. This is why surfacing and visualizing cyber risk is a key business function. Without doing so, there is no way to proactively protect the business against such threats.
How Do Third Parties Generate Cyber Risk

The Information Economy
Information is valuable, but it takes specialized work to extract that value from raw data. Many companies outsource information work such as analytics to other companies who specialize in that field. With this arrangement, companies are able to access the value of their data without dedicating a large resource base to it, while other companies are able to thrive solely by handling third party data. This widespread practice is especially prevalent at the largest scales of business, with some companies employing several information vendors at a time.

At this scale, datasets are typically extremely large, with millions of rows of information about as many unique individuals. The power of analytics emerges with large datasets, revealing trends, sectors, and areas for improvement. Often these datasets include sensitive customer information: personal details, Social Security numbers, credit card numbers, purchase and browsing history, credit reports, medical information, and so on.

Here’s the rub. When a company outsources information work, it also outsources the business risk of that information. The primary company can’t simply wash its hands and say “it’s not our fault,” because a vendor lost their data instead of an employee. Why not?

Trust Relationships
All business depends on trust. It is the cornerstone of trade, and without it, economy grinds to a halt. Businesses refer to “the brand” as the single entity a customer interfaces with when they enter this relationship. Internally, operations might be divided among several
company offices across the world, as well as numerous vendors and other third parties. But as far as the customer is concerned, there is only one indivisible entity with whom they are dealing: the brand.

When a third party data handler exposes the data of another company, it is the trust relationship between the customer and the primary company that is damaged. No explanation about outsourcing or vendors will change that. Whatever happens internally, inside the opaque edifice of the brand, is totally irrelevant to the customer. One need only examine social media outcry after a third party breach to understand this is so.

When a vendor mishandles data or is the victim of an attack, it is the relationship between the primary company and the customer that is breached and damaged.

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.

How to Protect Your Business From Third Party Risk

Limit Information Scattering
When risk enters the equation of analytics outsourcing, the first obvious way to reduce it is to limit that outsourcing as much as possible. Minimize the number of vendors who handle data, and restrict the dataset they receive to only what they need for the information work they’re doing. Sometimes this requires sensitive information, but sometimes it doesn't, and when it doesn't, the data should
be scrubbed appropriately instead of handed over in full, as often happens. Every copy of a production data set is a risk vector for breach. Outsourced information work is crucial to remain competitive, but it should be done with careful forethought to the risks the company faces should that information be compromised.

**How UpGuard Helps**
UpGuard acts as an inventory for your information and technology vendors, visualizing the business relationships your organization has formed with third parties so that everyone involved knows exactly who has access to your data, preventing redundant allowances and extraneous copies of the data set.

**Know Your Vendors**
Vendor consideration should involve cyber risk assessment, knowing their practices and profile, how they stack up against competitors, and what obvious threats they may be exposing your

---

**External Cyber Risk**

**Microsoft**

- **External Cyber Risk Score**: 689 / 950
- **Valuation**: $85B
- **Employees**: 131,287
- **Location**: Redmond, WA
- **CEO**: Satya Nadella, 95% Approval Rating

**Websites (8,000)**

<table>
<thead>
<tr>
<th>Web URL</th>
<th>CERAR Score</th>
<th>Cyber Trend</th>
<th>Date of Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Vendors**

<table>
<thead>
<tr>
<th>Vendor Name</th>
<th>CERAR Score</th>
<th>Cyber Trend</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---
information to. This due diligence can prevent a future breach. Like any sound business practice, you don’t want to enter into an agreement with someone you don’t know, and you don’t want to expose yourself to an unknown amount of risk in doing so.

For example, many information handling third parties host their (your) data in the cloud. The cloud is a great enterprise storage option, and when done correctly, offers immense value. But when done incorrectly, it can expose that data to the internet, as we saw in the real world examples above.

**But What Can You Know?**
Without being able to delve into a vendor’s internal infrastructure, there is only so much that can be independently known about their cyber risk profile. These are external factors, information that can be gleaned by anyone on the internet. While not a complete picture of the vendor’s total cyber risk, it does offer a facet of it, and usually those who are externally resilient follow suit with internal practices.

Have IT work with management to build a questionnaire or checklist that vendors must fill out before being hired. A combination of empirical data from external assessment and considered answers from the vendor should offer a much fuller picture of risk than going in blindly.

**How UpGuard Helps**
UpGuard assesses all of these external factors, and aggregates them into a single score between 0-950 called CSTAR. This allows you to understand at a glance a vendor’s external risk profile, and how they compare against similar companies.

UpGuard’s external scan examines, among other technical factors:
- Email settings to help prevent phishing scams
• Website encryption and best practices
• Outdated and vulnerable web server software
• Open ports, such as those through which ransomware propagates
• Company profile, including employee satisfaction and CEO approval
• Breach history and magnitude

All of these factors impact the risk a vendor poses when handling data. The CSTAR enterprise risk score allows executives to understand how third parties rate overall, while the external scan details help IT teams ask important questions and dig deeper into how the vendor keeps data safe. For example, your vendor questionnaire could include specific queries about external security practices discovered by UpGuard, giving your team more leverage than simply taking the vendor's word for it.

Establish a Risk Threshold
Once you have a standardized method by which to assess vendor risk externally, you can enforce a business policy that vendors must meet a certain threshold, or certain criteria, in order to handle your information. This way you can at least vett those vendors who lack external resiliency—a good sign that internal operations are also risky.

How UpGuard Helps
UpGuard gives businesses the data they need to make good decisions about vendors. By using UpGuard’s CSTAR risk score to judge vendors, it becomes very simple for companies to establish a policy that vendors must have and maintain a CSTAR score above a certain number to do business. Because not only should vendors be assessed before entering into an agreement, they should be continually assessed thereafter, to
ensure that they comply with your company standards as long as they have your data.

Furthermore, UpGuard provides detailed external profiles of vendors that your IT team can use to understand specific issues, such as what protections they have implemented against common cyber attacks, whether they have dangerous ports exposed to the internet, and whether their own website has the kind of controls in place to mitigate the risk of information mishandling. Finally, UpGuard can track vendor profiles over time and establish trends for improving or decreasing security posture, so your team can go in with hard data the next time a contract is up for renewal.

Holding information vendors to a standard of risk seems like an obvious business decision, but in practice many companies do not factor in vendor risk when engaging in third party data handling. Sometimes this process is siloed within IT, where other concerns are used as the criteria for vendor acceptance. The real question is: how much is your data worth? If it's worth analytical processing or other third party outsourcing, it's probably worth protecting, both internally and in the hands of vendors.

**Cyber Insurance**

Finally, as cyber risk gains more focus, insurance to help mitigate that risk will become more prevalent. Cyber insurance is already a somewhat common practice, but it has yet to develop into a mature field. One problem that insurers face when handling cyber insurance is scoping the insurance to a company's actual risk. Typically, factors like size,
industry, revenue, and other long-lived insurance criteria are used to gauge expectations.

However, future cyber insurance offerings are sure to rely on more specific criteria tied directly to the company’s digital footprint. An important part of this footprint will be the vendors used to handle information. Because when it comes to data breaches, history has shown that third parties are heavily involved. They are a major vector of risk.

**How UpGuard Helps**
UpGuard leads the way in enterprise cyber risk assessment, covering all aspects of the internal data center, the cloud, and vendors, to produce an accurate and meaningful risk score, with the technical details of the score available to IT staff so posture can be improved.
Conclusion

The information economy is booming, and won’t be slowing down soon. However, it is those companies who can take advantage of its value while staving off its risk that will succeed. Unaddressed risk will eventually lead to a major incident—data breach, cloud leak, business outage. These incidents damage customer trust, leaving companies scrambling to rebuild it, while instituting reactive cybersecurity policies at premium costs. Incorporating cyber risk into your everyday business operations allows you to understand it, and therefore proactively address it, before an incident occurs.

It can’t be overstated: one of the most common vectors of cyber risk is third party data handlers. If care is not taken in selecting them and continuously assessing their posture, it doesn’t matter what kind of defenses you’ve built for your company—your data is only as safe as the weakest link through which it passes.
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.