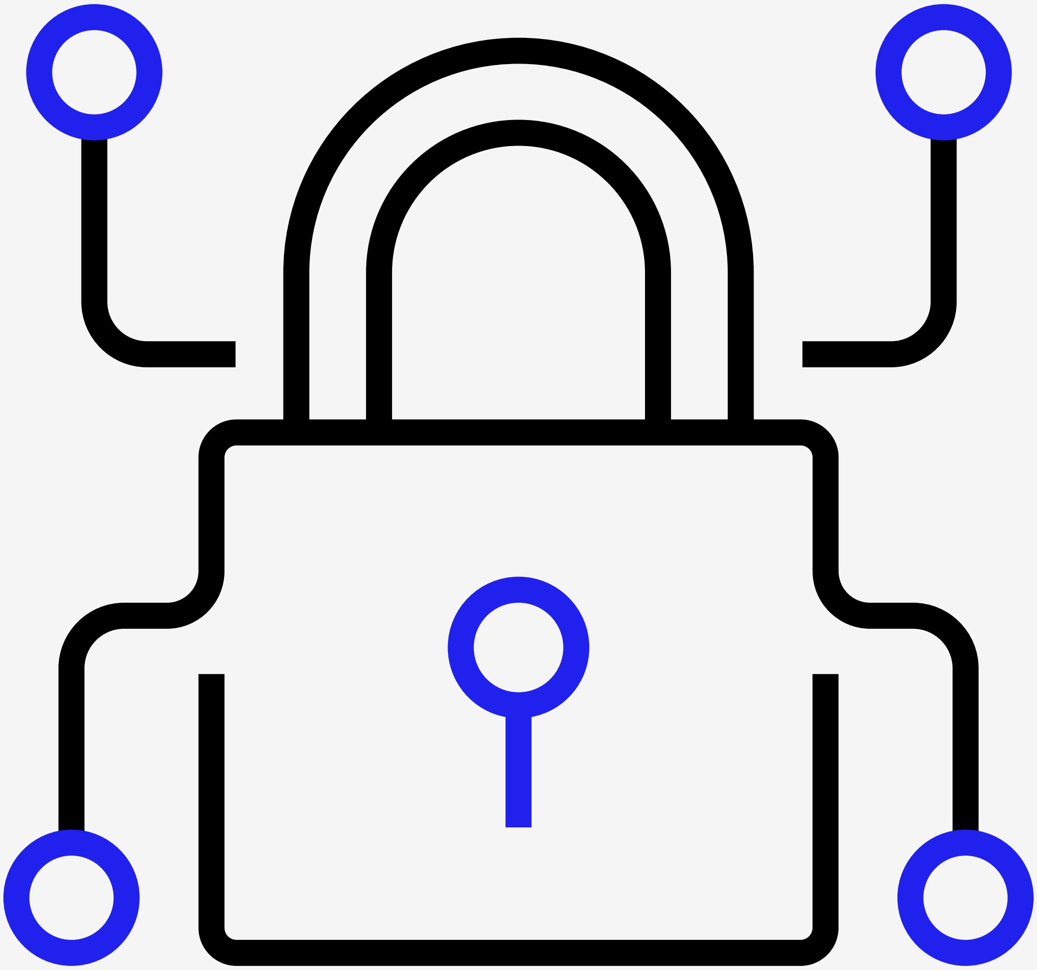
at bay

The Rise of Third-Party Risk — and How to Protect Your Business



at-bay.com

Table of Contents

Introduction

Businesses today are unfortunately faced with a new disheartening reality: Even if your organization is secure against cyberthreats, you can still become a victim of a cyberattack through the vendors and partners you work with. The growing reliance by businesses on technology products and services from other companies is making this risk more pervasive and increasingly damaging.

The term “third-party cyber risk” refers to the risk of data breaches, malware infections, and system disruptions stemming from any suppliers, vendors, customers, or business partners that have access to your organization’s networks, systems, or sensitive data, or those that provide IT products or services that your company depends on to operate.

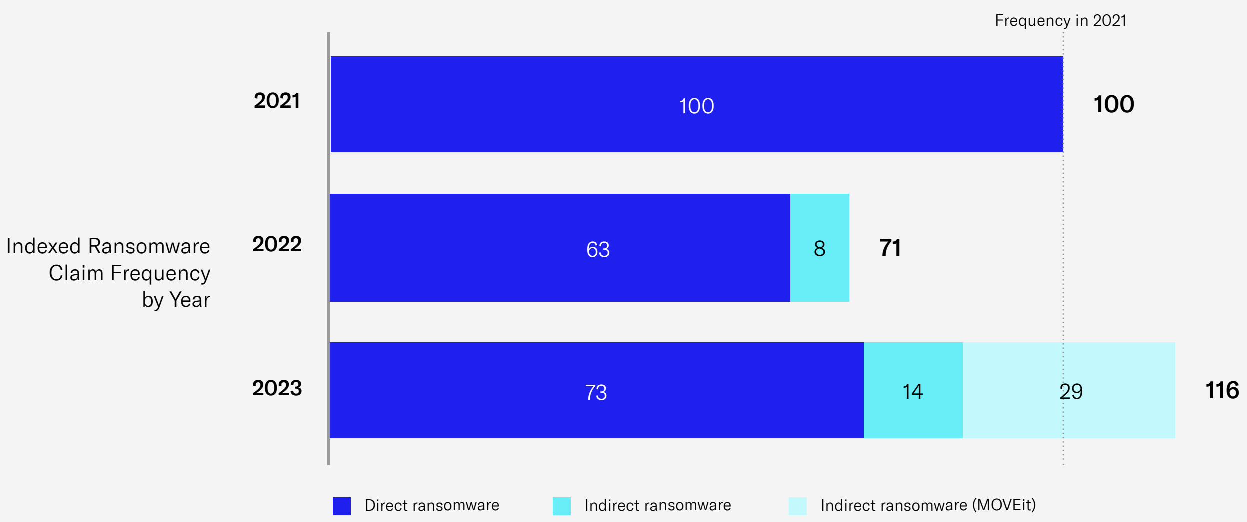
Here are some examples:

- A popular file sharing software frequently used by higher education institutions to share student profile information is breached by a cyberattacker. The attacker gains access to sensitive student data shared by one of those institutions, resulting in a widespread data privacy breach.
- A healthcare technology used to process insurance claims is hit by a ransomware attack, which shuts down its systems. Various medical practices reliant on this technology to process claims are unable to do so, resulting in business interruption losses.
- A car dealership software platform is downed by a cyberattack, leaving dealership sales reps across the country unable to access the systems they need to sell cars, causing significant loss in revenue.

None of these businesses in the examples above (higher education institutions, medical practices, car dealerships) were themselves directly attacked, but the vendors they used were. These are examples of how third-party risk manifests itself — and all of these stories are becoming more frequent and more severe.

In 2023, At-Bay saw a 415% increase in claims frequency for indirect ransomware (a ransomware attack on a vendor or partner of the primaryorganization that results in damages to the organization, typically data privacy breach and/or business interruption). For small and medium-sized businesses, these incidents can be an operational headache, not to mention costly, carrying an average claim severity of $47K in 2023[1].

Indirect Ransomware Frequency Increased 415% in 2023



Source: The 2024 InsurSec Report: Ransomware Edition, At-Bay 2024

Recent high-profile incidents, including those targeting MOVEit, Change Healthcare, and CDK Global, have demonstrated how a ransomware attack on a single vendor can create widespread downstream disruptions to the businesses that use that vendor.

[1] "The 2024 InsurSec Report: Ransomware Edition", At-Bay 2024

Attacks on industry-specific software products can create an outsized impact on their customers and partners

May 2023: **Progress MOVEit**	• Educational nonprofit National Student Clearinghouse attacked via MOVEit vulnerability • Impact: 890 schools breached
February 2024: **Change Healthcare**	• Ransomware attack resulted in a complete system outage of insurance processing • Impact: Estimated $100M per day revenue losses
June 2024: **CDK**	• Back-to-back ransomware attacks downed auto dealership software • Impact: $600M in losses

In each of these incidents, businesses reliant on MOVEit, Change Healthcare, and CDK were subject to financial losses, legal liabilities, and reputational damage — even though those businesses were not directly breached or attacked. This is the nature of the third-party risk introduced by vendors and partners, which is why organizations must now prioritize the identification, assessment, and mitigation of this potentially incapacitating risk.

This guide will provide the knowledge and strategies necessary to effectively identify and manage third-party cyber risks. By following the principles outlined in this guide, organizations can enhance their resilience against third-party risk to help safeguard their operations, data, and reputations.

Identifying Your Critical Third-Party Dependencies

The first step in mitigating third-party cyber risk is to identify your organization's critical third-party dependencies. "Dependencies" refer to the vendors, partners, and providers that are required for a company's operations — i.e., operations would cease if the vendor failed to deliver as agreed or suffered an outage of some kind.

Here are the steps to identifying your organization's critical third-party dependencies:

1. Understand Your Business's Value Chain

First, you need to outline your business's value chain, which is the sequence of activities required to deliver your product(s) or service(s) to your customers. Following is an example of what a value chain might look like and the potential vendors along that chain.

Customer Interface

How your organization interacts with and presents your products or services to your customers.

This could include websites, storefronts, or marketing channels.

Example vendors: Monday.com, Salesforce, Zendesk

Order Intake and Processing

How your organization receives and processes customer orders.

This could involve online ordering systems, call centers, or manual processes.

Example vendors: Microsoft 365, Netsuite, Coupa

Fulfillment

How your organization delivers your products or services to customers.

This could include inventory management, shipping, or service delivery platforms.

Example vendors: Shopify, Shipbob, Zoho Inventory

Invoicing and Payment

How your organization bills and collects payments from customers.

This could involve invoicing software, payment gateways, or traditional billing systems.

Example vendors: Square, Stripe, Helcim

Back-end Corporate Functions

How your organization manages internal operations like HR, payroll, and compliance.

This could involve specialized software or outsourced services.

Example vendors: ADP, Gusto, Workday

2. Identify Mission-Critical Functions Enabled by Third Parties

Once you have mapped out your organization's value chain, the next step is to identify which functions along that value chain are vital to keeping your business operational. Not all components of your value chain are equally critical; some may be more important than others. To determine which are critical, use the following table to go through your company's functions one by one to determine what the potential ramifications would be if you lost the ability to complete each of those functions.

If we lose...	... then we can't...	...which means we...
Access to our cloud-hosted email	Receive customer orders or platform customer service for in-progress orders	Lose revenue due to reputational damage and customer churn
Our insurance claim processing system	Process insurance claims related to products and/or services we've provided	Can't collect revenue
Our specialized, industry-specific platform that handles all business technology functions	Operate as a business	Lose current and future sales to competitors

After identifying your organization's mission-critical functions, determine which of these functions are enabled or performed by third-party products or services. These third-party dependencies are potential sources of cyber risk and should be prioritized for further evaluation and risk mitigation, which we'll explain in the following section.

3. Identify Functions That Lack Easily Sourced Alternatives

Not all third-party dependencies pose equal risk. To identify your company's high-risk dependencies, ask yourself the following questions for each mission-critical third-party function you have identified:

1. Which of our mission-critical functions are performed or enabled by a third-party product or service?

2. Which of those third-party vendors don't have existing or easily sourced alternatives?

By answering these questions, you can narrow your focus to the third-party dependencies that are essential to your business operations and lack readily available substitutes.

Next, it's important to prioritize these dependencies based on their potential impact on your business. Consider factors such as revenue loss, legal implications, and reputational damage in the event of a cyber incident or service disruption involving these third parties.

We've included a printable third-party risk assessment checklist at the end of this ebook for you to use with your team.

In addition, cybersecurity advisors can help you determine which functions are mission-critical to your organization, identify and prioritize your third-party risks, and provide actionable security recommendations. At-Bay Cyber and Tech E&O policyholders have access to At-Bay Stance™ Advisory Services , a team of cybersecurity experts who can assess and advise you on your cyber risk.

Schedule a call with At-Bay's Advisory Services team to get started.

[2] Access to At-Bay Stance Advisory Services is available to policyholders via the "Embedded Security" fee and the corresponding endorsement. Your Embedded Security Endorsement refers to "At-Bay Stance Advisory Services" as "At-Bay Stance Managed Security."

Evaluating Third-Party Cyber Risk

With your third-party dependencies prioritized, the next step is to thoroughly evaluate the cyber risks associated with each of your vendors or partners to determine appropriate risk mitigation strategies. This requires proper due diligence on all critical third-party vendors.

This due diligence process should be repeated periodically, ideally annually, to ensure that all third-party vendors' security controls and practices remain adequate.

10 Questions to Assess Third-Party Cyber Risk

To guide your due diligence efforts, make sure you can answer the following 10 questions:

1 **Does the vendor have industry-standard security controls in place?**

Ensure that the third party has implemented security controls that are appropriate for its industry and the level of risk it represents. This may include measures such as multi-factor authentication (MFA), data encryption, secure remote access, and regular vulnerability scanning.

2 **Does the vendor appear to have contingency plans that are sufficient to make it resilient to attacks?**

Cyberattacks are increasingly common, and no organization is immune. Evaluate whether the vendor has developed and tested incident response and business continuity plans to minimize the impact of a security incident and facilitate rapid recovery.

3

Is the vendor aware of its legal and contractual cybersecurity obligations to customers?

Many contracts include provisions related to data protection, breach notification, and other cybersecurity responsibilities. Ensure the vendor understands and adheres to these obligations, as its failure to do so could expose your organization to legal and financial risks.

4

Does the vendor have one or more industry certifications like SOC 2, HITRUST, etc.?

Industry certifications, such as SOC 2 (Service Organization Control), HITRUST (Health Information Trust Alliance), and ISO 27001 (Information Security Management System), serve as a useful shortcut to validate that a vendor has a slate of security controls in place and operational. These certifications demonstrate verification of security practices by an independent third party in writing.

5

Does your organization have a clear understanding of what data it shares with this vendor?

Identify the types of data, including sensitive information such as personally identifiable information (PII) or protected health information (PHI), that your organization shares with the third party. This will help you assess the potential impact of a data breach or unauthorized access.

6

Does your organization have a clear understanding of any technology integrations or access that it shares with this vendor?

If the vendor has direct access to your organization's systems or networks, ensure that you understand the extent of this access and the associated risks. Implement appropriate access controls (like MFA) and monitoring measures to mitigate potential threats.

7

What is the impact to your organization if this vendor experiences a security failure or outage?

Quantify the potential consequences of a third-party security incident or outage, including lost revenue, operational disruptions, legal implications, and reputational damage. This analysis will help you prioritize risk treatment strategies and allocate appropriate resources.

8

Has your organization identified alternatives to this vendor if/when they become necessary?

Explore the availability of alternative vendors or solutions that could be leveraged in the event of a security incident or prolonged outage involving the primary third party. Having backup options can enhance your organization's resilience and reduce the impact of a third-party failure.

9

What are the legal implications to your organization and its stakeholders if this vendor experiences a security failure or outage?

Explore the availability of alternative vendors or solutions that could be leveraged in the event of a security incident or prolonged outage involving the primary third party. Having backup options can enhance your organization's resilience and reduce the impact of a third-party failure.

10

What recourse does your organization have in the event of a security failure or outage with this vendor?

Explore potential remedies, such as cyber insurance coverage, contractual indemnification clauses, or legal action, that could help your organization recover from losses or damages resulting from a third-party incident. Ensure that these remedies are clearly defined and understood by all parties involved.

By thoroughly evaluating third parties using these questions, you can gain valuable insights into the potential threats and vulnerabilities associated with each of your critical vendors and partners. This knowledge will inform your risk mitigation strategies and help you prioritize your efforts to mitigate third-party cyber risks effectively.

Controlling and Mitigating Third-Party Cyber Risk

A thorough due diligence process should eliminate the majority of third-party cyber risk by removing high-risk providers from consideration in the first place. Still, the residual risk among the remaining providers must be managed continuously and actively by your organization.

Following are various approaches to effectively manage and reduce the potential impact of third-party cyber incidents on your organization, including dependency elimination and contingency planning.

Source Alternative Vendors

One of the most effective ways to control third-party cyber risk is to have alternative vendors in place for your critical dependencies. This approach provides redundancy and reduces the impact of a single vendor's security failure or outage. By maintaining relationships with multiple vendors for the same service or product, you can quickly switch to an alternative provider if needed. Remember, having an alternative provider is only necessary for the most business-critical operations.

However, it's important to note that sourcing alternative vendors may not always be feasible or practical, especially for highly specialized services or products. In such cases, you may need to explore other risk mitigation strategies in the following section.

Insource Critical Functions

In some situations, it may be more appropriate to bring certain critical functions back in house rather than relying on third-party vendors. This approach, known as insourcing, can provide greater control over security measures and reduce the risk of third-party cyber incidents.

Insourcing critical functions can be particularly beneficial for organizations that handle sensitive data or have unique operational requirements. However, it's important to carefully evaluate the costs, resources, and expertise required to insource these functions effectively.

Develop Contingency and Business Continuity Plans

Even with alternative vendors or insourced functions in place, it’s crucial to have robust contingency and business continuity plans to mitigate the impact of third-party cyber incidents. These plans should outline specific steps to be taken in the event of a security breach, system outage, or other disruptions caused by a third-party vendor.

Contingency plans should address various scenarios like data loss, system downtime, and communication disruptions and should include procedures for quickly restoring critical operations, minimizing financial losses, and maintaining customer trust.

Business continuity plans should focus on ensuring the long-term resilience and continuity of your organization’s operations in the face of significant disruptions. These plans should cover strategies for maintaining essential functions, recovering data and systems, and resuming normal operations as quickly as possible.

Continuous Monitoring and Management

Because mitigating third-party cyber risk requires ongoing monitoring and management, you'll need to establish a process to continuously assess third-party risks and maintain a proactive stance against emerging threats. Here are the crucial components to a comprehensive risk management program:

Establish a Risk Reassessment Cadence

One of the most important aspects of ongoing risk monitoring is setting a regular cadence for reassessing your third-party cyber risks. Many organizations make the mistake of evaluating their vendors and partners only during the initial onboarding process, failing to account for changes in the vendor's security posture or the introduction of new threats over time.

> An annual reassessment is generally recommended as a minimum frequency, but the optimal cadence may vary depending on the criticality of the third-party relationship and the vendor's industry or risk profile.

For example, vendors handling sensitive data or operating in high-risk industries — such as those that handle payment information or those that store or process unencrypted sensitive data — may warrant more frequent reviews, such as quarterly or biannually.

During these reassessments, it is essential to revisit the due diligence process outlined in Chapter 2, including evaluating the vendor's security controls, certifications, and contractual obligations. Additionally, you should review any changes to the data or technology integrations shared with the vendor and reassess the potential impact of a security incident or outage.

Work with Cyber Advisors

Some InsurSec providers, like At-Bay, offer cyber advisory services and risk assessment tools to help policyholders identify and mitigate third-party cyber risks. By leveraging these resources, you can gain a deeper understanding of your organization's specific risk exposure and develop tailored mitigation strategies without stretching the bandwidth of your in-house teams.

Additionally, cybersecurity advisors and consultants can provide expert guidance on industry best practices, emerging threats, and effective risk management techniques. Their expertise can be invaluable in interpreting risk assessment results, developing contingency plans, and implementing robust security controls within your organization and across your third-party ecosystem.

Continuous collaboration with these partners can help you adapt your risk management strategies to changing circumstances and maintain a proactive stance against third-party cyber risks.

What is InsurSec?

Cybersecurity should provide safety businesses can count on, but modern solutions are too expensive, too hard to purchase, and too difficult to manage. This leaves many businesses unsure how protected they are from an attack and only relying on cyber insurance to help them recover after an incident.

That's why At-Bay brings together cybersecurity and cyber insurance in the world's first InsurSec solution. This closed-loop system uses real-world cyber insurance claims data to inform security recommendations, delivering end-to-end prevention and protection. Insursec not only keeps businesses safer, it also helps them reduce their risk profile and, in turn, unlocks better insurance terms and pricing.

Learn more at at-bay.com

Leverage Third-Party Risk Management Tools and Services

To streamline the continuous monitoring process and enhance its effectiveness, consider leveraging third-party risk assessment tools and services. These solutions can automate various aspects of vendor risk management, including:

Vendor risk profiling
These tools can help you gather and analyze relevant information about your vendors, such as their security practices, certifications, and industry ratings.

Continuous monitoring
Some tools offer ongoing monitoring of your vendors' security posture, alerting you to potential risks or changes that may require further investigation.

Risk scoring and reporting
Many solutions provide risk scoring mechanisms and reporting capabilities, enabling you to prioritize and communicate third-party risks effectively.

Vendor risk assessment questionnaires
These tools can facilitate the distribution, collection, and analysis of standardized security questionnaires to your vendors.

While these tools can help you streamline the information-gathering process, it is essential to interpret the results with the guidance of cybersecurity professionals. Vendors' responses to questionnaires or self-reported information may not always provide a complete picture of their actual security practices.

Protect Yourself with Cyber Insurance

One of the best protections against a potentially incapacitating third-party cyberattack is cyber insurance. With the right coverage, cyber insurance policies can provide financial protection against losses resulting from third-party cyber incidents on a vendor, such as data breaches, system outages, and ransomware attacks.

It's crucial to work closely with your cyber insurance provider to ensure that you have the appropriate coverage for your organization's specific needs and third-party dependencies. Some InsurSec providers offer security services as part of their insurance policies. At At-Bay, this includes cyber advisory services and active risk monitoring.

Third-Party Risk Management: A Critical Component of Your Cybersecurity Strategy

Direct observation, measurement, and control of third-party cyber risks remain elusive. In spite of the expansive availability of cybersecurity solutions, there still aren't tools available that can surface value chain dependencies, evaluate contract language, or predict the future – much less all three at once. Thus, businesses continue to have a need for human attention, analysis, and intervention.

By adopting a few straightforward practices, your businesses can minimize and mitigate its third-party risk. The application of vendor due diligence, dependency breaking, and contingency planning together – with the support of cyber advisors who can lend their expertise in evolving threats and risk management– can significantly reduce the risk that you will become a victim of other companies' security failures.

At-Bay Cyber and Tech E&O policyholders have access to At-Bay Stance Advisory Services[3], a team of cybersecurity experts who can assess and advise you on your cyber risk. Schedule a call with At-Bay's Advisory Services team to get started.

Contributing Expert

Adam Tyra
GM, Security Services

Adam Tyra is a technology professional with over 18 years of experience in security and deep expertise in cybersecurity operations. He currently serves as At-Bay's General Manager of Security Services. Prior to joining At-Bay, Adam was a security leader at Kivu Consulting, TalonX, McKinsey & Company, and EY. Before becoming a consultant, he worked as a software developer, architecting and implementing cybersecurity tools for the U.S. defense and intelligence communities. He also served as a cyber security officer in the U.S. Army.

[3] Access to At-Bay Stance Advisory Services is available to policyholders via the "Embedded Security" fee and the corresponding endorsement. Your Embedded Security Endorsement refers to "At-Bay Stance Advisory Services" as "At-Bay Stance Managed Security."

About Third-Party Risk for Businesses

Third-party risks are the risks to a business stemming from anything that a supplier, vendor, customer, or business partner does or fails to do.

Third-party risks aren't new. But, the increasing reliance by businesses on technology products and services from other companies is. At-Bay's 2024 InsurSec Report found indirect ransomware (an incident where an organization is indirectly impacted by a cyber event on their vendor or partner), exploded by 415% in 2023.

This situation has led to increased risk for businesses and warrants an assessment and understanding of such risks as part of ongoing business continuity planning and risk management procedures.

About At-Bay

At-Bay is the InsurSec provider for the digital age. By combining world-class technology with industry-leading insurance and security expertise, At-Bay was designed from the ground up to empower businesses of every size to meet cyber risk head on.

The At-Bay Group includes a cybersecurity company and a full-stack insurance company. As an insurance company, At-Bay offers Cyber, Tech E&O, and Miscellaneous Professional Liability policies.

At-Bay's InsurSec approach provides end-to-end protection for modern businesses. It's a force multiplier that includes security, threat intelligence, and human experts to close the SMB cybersecurity gap — all as part of their insurance policy.

* Access to At-Bay Stance Advisory Services is available to policyholders via the "Embedded Security" fee and the corresponding endorsement. Your Embedded Security Endorsement refers to "At-Bay Stance Advisory Services" as "At-Bay Stance Managed Security."

Third-Party Risk Assessment Checklist

Vendors that are or will be critical dependencies in a company's value chain should receive an appropriate level of scrutiny before being engaged. Here are a series of questions to ask these vendors to assess what level of risk they may pose to your business operations.

How to use this document

1. Identify your business's mission-essential functions and processes
2. Identify which mission-essential functions are performed or enabled by a third-party product or service
3. Identify which third-party products or services don't have existing or easily-sourced alternatives
4. For each of the third-party products or services in your list, answer the below questions

At-Bay cyber insurance policyholders may have access to At-Bay Stance Advisory Services*. This is a team of advisors who can help review your third-party risk assessment, identify your risk, and discuss recommendations.

Schedule a call with At-Bay's Advisory Services team for your assessment.

MISSION-ESSENTIAL FUNCTIONS	PRODUCT OR SERVICE THAT ENABLES THE MISSION-ESSENTIAL FUNCTION	IS THERE AN EASILY-SOURCED ALTERNATIVE?
EXAMPLE Insurance Claim Processing	Change Healthcare	□ YES □ NO
		□ YES □ NO
		□ YES □ NO
		□ YES □ NO
		□ YES □ NO
		□ YES □ NO

MAKE A COPY OF THIS WORKSHEET FOR EACH MISSION-ESSENTIAL VENDOR

QUESTIONS	NOTES
Does the vendor have industry-standard security controls in place?	
Does the vendor appear to have conducted their own contingency planning sufficient to make them resilient to attack?	
Is the vendor aware of their legal and contractual obligations to customers for cybersecurity?	
Does the vendor have one or more industry certifications such as SOC 2, HITRUST, etc.?	
Do we have a clear understanding of what data we share with this vendor?	
Do we have a clear understanding of any technology integrations or access that we share with this vendor?	
Have we identified alternatives to this vendor if / when they become necessary?	
What is the impact to our organization if this vendor experiences a security failure or outage?	
What are the legal implications to us and our stakeholders of a security failure or outage with this vendor?	
What recourse do we have in the event of a security failure or outage with this vendor?	

This document is intended for information purposes only and does not modify or invalidate any of the provisions, exclusions, terms or conditions of the policy and endorsements. For specific terms and conditions, please refer to the coverage form. At-Bay Insurance Services LLC is a licensed insurance agency and surplus lines broker in all fifty states and the District of Columbia. ©10/2024 At-Bay. All Rights Reserved.