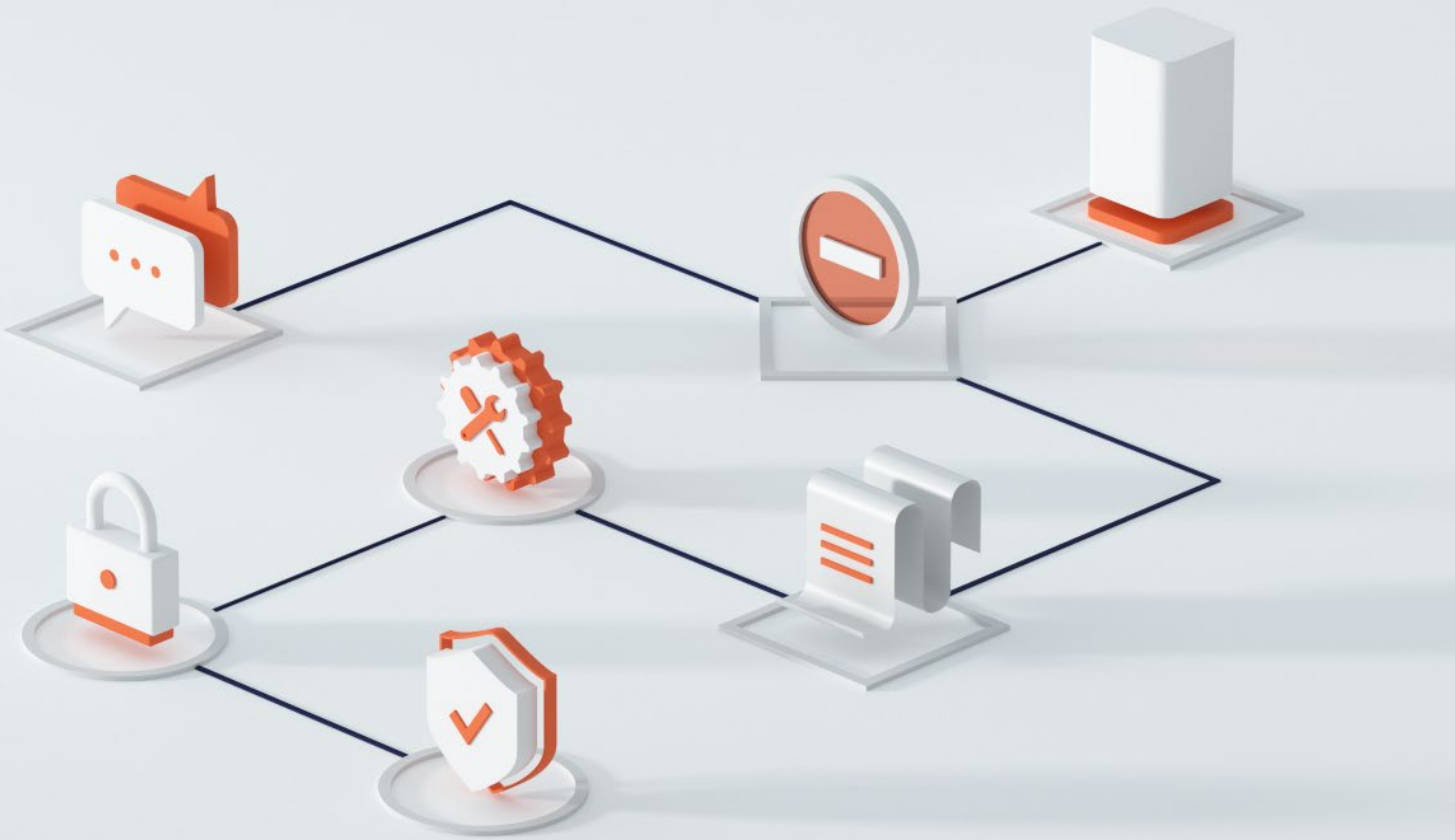
Panorays

The Third-Party Incident Response Playbook

A practical guide to protecting against and preparing for a possible vendor cyber breach



Contents

Before You Get Started

Most companies work with an average of 583 vendors, according to a Ponemon Institute study [1]. Have you thought about what could happen if one of those vendors was breached and the impact that would have on your business? Have you considered what your response would be if your organization was the victim of a cyberattack through one of your third parties?

This Third-Party Incident Response Playbook was created to help people like you, who have been charged with the critical responsibility of keeping your organization's data secure at a time when third-party breaches are on the rise. This playbook will help you:

- Understand why third-party security is critically important
- Prepare for a possible supply chain cyberattack
- Recognize signs that may indicate a possible third-party cyberattack
- Respond and recover from such an attack

[1] Ponemon study. *Data Risk in the Third-Party Ecosystem.* 2018.

II Executive Summary

With third-party security incidents growing exponentially, companies must prepare for the worst. According to a recent Deloitte survey, 83% of organizations have suffered a breach at the hands of a third party within the past three years. So it's no wonder that CISOs and security professionals are quickly prioritizing third-party security management.

In reality, your organization's cybersecurity controls are only as strong as the weakest link in the supply chain. Cybercriminals frequently target key suppliers or vendors of a company in lieu of the target company itself. The reason is simple; a small business providing a product or service to larger enterprises is often more vulnerable than the primary target. So it's easier for the cybercriminal to infiltrate the target organization's systems and data via third-party vendors, who typically have fewer security roadblocks than the larger organizations they service, and who may also be holding some or all of the organization's data.

According to a 2019 Deloitte poll[2], 70% of respondents have a moderate to high level of dependency on external entities such as third and fourth parties. A 2020 Deloitte report[3] finds that organizations' dependence on their third parties is only increasing as companies' reliance on vendors isn't just for cost saving or other short-term goals, but also to meet strategic objectives.

However, as enterprises' dependency on third parties continues to increase, so have the risks associated with the possibility of a digital supply chain attack. When working with more third parties, the perimeter that was once just your data center expands to include all of your third parties that have access to your data. This means your attack surface expands to include all of those third parties as well. And with supplier numbers in the hundreds, if not thousands, organizations likely have vendors that do not meet their internal security controls, regulations or risk appetite.

Clearly, the digital supply chain can be an organization's weakest link. Nothing drives home that point more than recent large-scale supply chain cyberattacks on Microsoft Exchange, Accellion, SolarWinds, Codecov and more. These notable attacks have sent cybersecurity professionals and business owners alike a strong and harrowing message—no company is immune.

Since no organization is exactly alike and no security incident is identical, responses to third-party security breaches will vary. That's why we created this playbook: to give organizations like yours a high-level incident response plan. It delves into why vendor security is imperative for your organization and provides clear and actionable steps to prepare for and respond to the ongoing threat of third-party security attacks.

---

[2] Deloitte poll. *Reestablishing the Perimeter.* 2019.

[3] Deloitte survey. *Third-party risk management global survey 2020.*

III Why Third-Party Security is Critically Important

While your company's cyber posture may be strong, this does not mean that you are immune to attackers. In fact, hackers typically target a company's weakest link, and a less-secure third party is the perfect conduit for cybercriminals to gain access and wreak havoc on your systems and data. Here are the main reasons why vendor security must prioritized in your organization:

01 Digital supply chain complexity

In today's hyper-connected world, organizations do business with lots of vendors. In addition, supply chains are so complex that many organizations are not even fully aware of who all their business partners are. This creates a clear problem: How do you protect your data if you don't know who has access to it?

As the supply chain continues to grow, organizations are realizing that they need help managing the security of the hundreds or even thousands of third parties they connect to. To achieve this, it's important to uncover all supply chain relationships by using an asset discovery tool that does continuous reconnaissance and to assess and continuously monitor all vendors. By doing so, organizations can pinpoint any security issues within the supply chain that can be fixed before cybercriminals exploit them.

02 Remote working

Since COVID-19, many companies—including third parties—have implemented work-from-home policies. This shift has created numerous significant cybersecurity issues.

As emails and online requests increase for charitable donations and other assistance since the pandemic began, there's also a greater risk of phishing and malware attacks. In addition, employees who use their own devices for work may also be engaging in less secure behavior on those same devices, such as downloading apps and kids' games, which may be infected with malware.

These risks can be even worse within the supply chain, particularly among smaller vendors that may lack the resources to implement the necessary security measures to monitor their employees' behaviors and access points. This presents an unfortunate opportunity for cybercriminals, who can target the employees of third parties to penetrate their upstream partners.

03 Cloud storage

With an increased usage of SaaS apps and data stored in the cloud, we will likely see even more disastrous data breaches resulting from cloud configuration mishaps or improperly secured (and sometimes even non-secured) servers. We saw these types of data leaks involving companies such as LightInTheBox, PayMyTab and OptionWay, illustrating what can happen when data is stored on insecure servers hosted by third parties.

This situation can be avoided by putting more emphasis on controlling access to system images and database backup files. Extra vigilance, however, is required to ensure that third parties store data securely. As organizations continue to store more data on the cloud through third parties, they are looking for solutions to check for cloud security.

04 Data privacy regulations

GDPR and CCPA have ramped up data privacy enforcement in the European Union and California, respectively, and similar regulations are being written and enacted throughout the world. These regulations are having a significant effect on how organizations approach managing privacy and vendor security.

The stakes are high for companies that don't comply with these regulations. GDPR noncompliance could result in penalties as high as €20 million or 4% of annual revenue—whichever is greater. With CCPA, organizations can be fined up to $2,500 for each negligent violation and up to $7,500 for each intentional violation. CCPA has a notable added consequence: Individuals can also seek damages of between $100 and $750, and actions can be aggregated into a class action. This leaves companies open to the possibility of enormous financial penalties through its users.

Organizations therefore have good reason to comply with these regulations, and cybersecurity plays a key role. GDPR demands that organizations tighten their cybersecurity—as well as their third parties'—to protect data privacy. CCPA similarly stipulates that organizations must implement "reasonable" security measures.

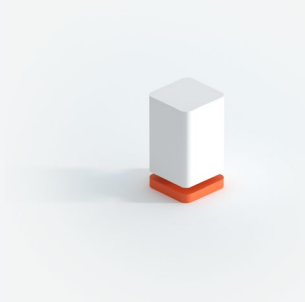
For all of these reasons, proper security vendor management is critical and organizations are searching for solutions to do it effectively and comprehensively. The best solutions will also offer a way to check CCPA and GDPR compliance, as well as checking cyber posture.

05 Phishing and ransomware attacks

Both phishing and ransomware attacks continue to be widespread. Not only are they quite effective, easy to create and yield quick financial rewards, but the widespread transition to remote work during the COVID-19 era also provided cybercriminals with a plethora of new tactics to take advantage of a vulnerable situation.

Phishing, which is an attempt to deceive a victim to gain access to confidential information and/or distribute infected files, has become one of the most widely used attack vectors among cybercriminals. In fact, 22% of all data breaches in 2020 involved phishing attacks. Ransomware, which is a type of malware that prevents users from accessing data until they pay a ransom, was reported[4] to cost US businesses more than $7.5 billion in 2019. In 2020, a staggering 51% of businesses were impacted by ransomware.

Often, the best way for cybercriminals to steal data from organizations is by targeting the employees of less-secure third-party vendors. Thus the ongoing and very real threats of phishing and ransomware are powerful motivators for organizations to implement a robust third-party security process.



Comprehensive Third-Party Security Management

Companies using Panorays gain continuous visibility and actionable insights into evolving supplier risk. The platform ensures vendors align with industry regulations, security controls and your company's risk appetite. Moreover, it's the only platform that considers the effect of human behavior when calculating cybersecurity ratings, checking the likelihood of the vendors' employees to be targeted for an attack based on factors such as social media presence, employee security awareness and having a dedicated security team.

Now that we have established the "WHY" behind third-party security, we can proceed to "HOW" vendor security can be achieved. The next section in the playbook discusses what your organization should do to protect its assets and how to prepare for potential threats posed by your third parties.

[4] Emsisoft Malware Lab. *The State of Ransomware in the US: Report and Statistics 2019.*

IV Preparing for a Possible Third-Party Breach

The infamous SolarWinds third-party security breach was a huge wake-up call to organizations worldwide. If a large and well-known company like SolarWinds could be breached, so could any organization.

SolarWinds was compromised when hackers, believed to be Russian, inserted malware and malicious code into its "Orion" network management product updates. As a result, 18,000 organizations may have installed the software and been compromised. These include the U.S. Treasury Department, the U.S. Department of Homeland Security and cybersecurity firm FireEye.

Though SolarWinds was an extremely sophisticated attack, carried out by a seasoned cybercriminal that likely could not have been predicted or prevented, there are a number of important takeaways from this cyber incident. Taking proactive measures today will enable you to quickly and comprehensively respond to, remediate and recover from a third-party or digital supply chain breach.

01 Build cyber resilience and recovery

To achieve cyber resilience and recovery, you first must understand what your assets are. While servers and system components are certainly assets, so is any entity that processes or holds your data. Therefore, external third-party services and tools/SaaS apps that process or hold your data should also be included as assets.

Examples include, but are not limited to:

- Internal servers protected by VPN
- Email services
- Marketing tools
- Customer success tools
- Hosting providers
- Cloud infrastructure providers

Given the heavy dependence on and growing number of third parties, it is imperative to map your vendors. Since many small security teams are charged with a multitude of responsibilities, and just one of those tasks is managing third parties, automation can help streamline and accelerate that lengthy and tedious process.

Without automation, it is nearly impossible to properly manage all of your vendors to the depth and breadth that is required to properly ascertain their security posture. Automation also enables a more expansive discovery phase, giving you more visibility and understanding of which assets need attention.

02 Identify important assets

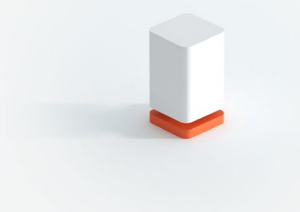
Now that you've identified your assets and those of your third parties, you need to prioritize them. Though challenging, it is critical to keep track of your attack surface that has expanded to include whoever holds or processes your data (data at rest and data in transit).

Creating an inventory that includes your physical infrastructure as well as your virtual infrastructure (your vendors) is a solid foundation for securing your assets. Once you have identified and prioritized your assets, you must establish a system to monitor all of these assets, creating visibility of their dynamic and changing landscape.

03 Reduce third- and fourth-party security risk

As discussed earlier, you utilize third parties for a variety of services. Each third party has its own infrastructure and its own third parties, which are your fourth parties. For this reason. it's incumbent on organizations to also understand fourth-party risk for parties handling your data.

A cyberattack could result in a breach within either your third or fourth party (or both, like the SolarWinds attack). While SolarWinds' customers were concerned about their data being compromised, organizations that have a vendor relationship with a SolarWinds customer were similarly distressed about the security of their own data. A big takeaway from this security incident is just how important it is to manage and mitigate third- and fourth-party security risk.



Understanding Your Third-Party Security Risk

Clearly, having visibility into and control over your third-party security is critical to maintaining a strong cyber posture and being proactive in the event of a vendor security breach. That's why Panorays combines automated, dynamic security questionnaires with external attack surface assessments and business relationship context to provide you with a rapid, accurate view of supplier and fourth-party cyber risk.

V The Signs and Signals You Should Watch Out for

While you may not be able to determine whether your third parties have experienced a cyber breach, there are certain signals that may indicate something is suspicious and should be examined. A reliable security ratings tool should alert you of such changes with your vendor:

New critical vulnerabilities (CVEs)

When a new critical finding is listed, it means that there are more security gaps to contend with. With this knowledge, you can notify the relevant vendor to remediate the vulnerability and follow your company's internal controls to manage the security risk.

Security ratings drop

When a vendor experiences a drop in security ratings, it's time to have a closer look and understand what precipitated the lower rating. Was something potentially dangerous found in its external digital footprint? Was it triggered by an answer in a security questionnaire that doesn't fit with your organization's risk appetite?

Increase in dark web mentions

If there is malicious chatter about opportunities to target your vendors on hacker forums and other nefarious marketplaces, you want to alert your third parties of these dark web mentions so they can take precautionary measures.

Increased mentions of a vendor being breached

When a vendor breach is repeatedly discussed in the news, it may be cause for concern. Even if you don't use that particular supplier, your vendors might, making the breached vendor your fourth party. Researching a high-profile breach is always recommended.

How Panorays Helps You See the Signs of a Possible Breach

The Panorays platform non-intrusively evaluates your vendor's attack surface through the analysis of externally available data. The platform continuously monitors and evaluates the supplier, and you receive live alerts about any security changes or breaches to your third parties. This rating, together with other factors like Panorays' Smart Questionnaires™, allows you to make informed security decisions regarding your third parties. With Panorays, you'll receive a notification when there is abnormal activity on the dark web regarding your supplier, as well as updates about high-profile vendor breaches that can affect your organization and warrant deeper investigation.

Even when you've done everything you can to reduce the inherent risks of working with other companies by bringing them into alignment with your own security policies, compliance regulations and risk appetite, there will unfortunately always be some risk of digital supply chain attacks.

While international standards such as ISO 27001 offer a framework to help companies manage and optimize their information security management systems, the NIST Cybersecurity Framework also offers us a guideline on how to respond and recover from security events.

How to Respond to a Breach

One day it will happen. Your third-party vendor has been breached; now what?

The most critical thing to do upon discovering your supplier has suffered a breach is to limit the damage on your organization by implementing the following measures:

01 Limit access and explore impact

Limit that third party's access to your systems, network and applications and determine whether the third-party breach has affected your organization. If it has, your next step is to conduct forensic analysis to understand the extent of the incident and its impact.

02 Mitigate damage and preserve evidence

Mitigate the damage through additional security tasks and tools to minimize any further incursion into your network, applications and systems. Sometimes that means unplugging systems, cutting off access, updating security policies (including access) and implementing new tools and protocols. One key consideration in this step is preserving evidence in the case of a later investigation by law enforcement.

03 Communicate with stakeholders

Communicate to stakeholders what has happened, the impact and your plan for recovery. A key part of this step is to have already thought through who needs to know about the event. First and foremost, speak with the vendor directly. Find out as many details about the breach as possible.

Though it sounds obvious, unfortunately something as simple as knowing who to contact and how to contact them in the event of a breach is often overlooked. Time is of the essence during a cyberattack, so having all the appropriate contact information lined up ahead of time can allow you to swiftly respond and react appropriately. Be sure to communicate with key internal contacts beyond the initial response team, such as members of the executive team, board of directors and employees as well as external audiences such as law enforcement, outside counsel, etc.

- It's important to note that if the incident involves the theft of personally identifiable data, there are state and federal requirements for issuing breach notifications. Know your legal obligations ahead of time.

04 Document responses and audit process

Document the organization's response to your vendor's breach, which can be used as a template for the next event—what worked, what didn't, what improvements are needed and the plan for implementing them next time.

Be sure to include important information such as:

- Whether or not your organization was or was not compromised and to what extent
- What actions were taken in the event that you were breached
- What was done to mitigate the risk

Having all this information documented will prove beneficial for you as an organization, as well as for any future audits performed on your company.

VII Recovering from a Breach

Once the incident is contained, it is time to think through how to return to normal business operations as quickly as possible. This could include not just restoring systems, but also the services associated with them, as well as planning how to better bullet-proof them against future incidents. This is known as cyber resilience.

While there will never be a 100% guarantee against future breaches, taking what you learned from the breach and bolstering your defenses is never a bad idea. According to the NIST Cybersecurity Framework, to "recover" after a breach means to "develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event."

During this stage, update your incident response plan to include recovery planning, improvements and communications.

Recovery planning
In order to mitigate the effects of a cyber breach as soon as possible, recovery plans should be tested, executed and maintained.

Improvements
If you want your recovery planning and processes to improve following cyber events, it is imperative that you identify the areas that fall short and propose new processes, operations and solutions for the future.

Communications
It is very important that information about the ongoing recovery efforts and progress during a breach recovery is communicated with both internal and external audiences; i.e. within your organization as well as with your customers and the market at large.

Following an attack, the recovery stage is not just about getting your organization back to business as quickly and as safely as possible, it is also an opportunity to build confidence with your customers. By having processes in place, communicating proactively and honestly with your customers and having a thought-out and detailed plan in place, you are not only building resilience, but also building business relationships.

Building Cyber Resilience
It is imperative to have an ongoing, comprehensive understanding of your suppliers' risk in order to properly manage it. Panorays is the only platform that automates, accelerates and scales customers' third-party security evaluation and management process, enabling easy collaboration and communication between companies and suppliers, resulting in efficient and effective risk remediation in alignment with your security policies and risk appetite.

Conclusion

Third-Party Security is Key to Managing Cyber Risk and Reducing Breaches

Given that the majority of data breaches start with third parties—because they are often easier to infiltrate than larger organizations—it's important to understand exactly who you are doing business with, what their security posture is and whether it is acceptable to your company. An unknown, incomplete or inaccurate view of supplier risk leaves your organization vulnerable. In other words, you must have visibility into and control of third-party security. Panorays quickly and easily automates third-party security risk evaluation and management—handling the whole process from inherent to residual risk, remediation and ongoing monitoring.

Would you like Panorays to help create a third-party incident response playbook and program for your organization?

Contact us for more information >

Panorays

Third-Party Incident Checklist

About the checklist

Wondering where to start to build your Incident Response Plan? Use this checklist as a guide to help your organization respond to a third-party security incident.

Since no organization is exactly alike and no security incident is identical, responses to third-party security breaches will vary. However, this checklist provides an overview of the relevant steps your organization should take in case of a third-party security breach.

This document should be filled out, per vendor incident, and updated on an annual or semi-annual basis (based on the vendor relationship) by an information security professional in your organization.

Authorized & updated by:	Version	Date

Use this table to list all **internal** parties involved in mitigating risk in your organization.

Title	Name	Phone	Email
VP R&D (Engineering Manager)			
CTO			
CISO (InfoSec Manager)			
CIO			
Legal			
DPO (Data Privacy)			
Procurement			
Business Owner/ Relationship Manager			
IR Team Contact			
Other			

Use this table to list relevant **internal** parties who need to be notified about security incidents:

Title	Name	Phone	Email
CEO			
COO			
Board of Directors #1			
Board of Directors #2			
Regulation Officer (as needed) #1			
Regulation Officer (as needed) #2			
Regulation Officer (as needed) #3			
Legal Contact			

Regulations may require reporting a security breach within a certain amount of time.

Document relevant **regulation** information here:

Regulation name	Required time to report a breach

Use this table to list relevant contacts for the specific **vendor involved in the incident** here:

Name of Vendor			
Title	**Name**	**Phone**	**Email**
CISO			
InfoSec			
Legal			
Business Owner/Relationship Manager			

PREPARATION

DETECTION & ANALYSIS

- ☐ Determine whether the third-party breach has affected your organization
- ☐ Limit third party's access to your systems, network and applications
- ☐ Conduct forensic analysis to determine the incident's impact
- ☐ Save all logs and documentation of the forensic information in a centralized place

CONTAINMENT

- ☐ Minimize further incursion into your network, applications and systems
- ☐ Unplug systems, cut off access and update security policies (including access), if necessary
- ☐ Implement new tools and protocols, as needed

COMMUNICATION

- ☐ Speak with the vendor who was breached and glean information
- ☐ Inform stakeholders of breach, its impact and recovery plan
- ☐ Inform executive team, board of directors and employees
- ☐ Inform relevant state and federal organizations as required

DOCUMENTATION

- ☐ Document your organization's response to the vendor breach
- ☐ List what was compromised and to what extent, if relevant
- ☐ Elaborate on actions taken following the breach
- ☐ Explain what was done to mitigate the risk
- ☐ Preserve evidence for future reference/audit

RECOVERY

- ☐ Restore systems and associated services
- ☐ Update incident response plan: recovery planning, improvements and communications
- ☐ Test, execute and maintain recovery plans
- ☐ Identify issues and propose new processes, operations and solutions
- ☐ Maintain ongoing communication with internal and external audiences about recovery
- ☐ Improve business relationships through proactive and honest communication

If you have questions about this Third-Party Incident Checklist or need assistance related to your Third-Party Incident Response Program, **contact Panorays for more information >**

About Panorays

Panorays is a rapidly growing provider of third-party security risk management software, offered as a SaaS-based platform. The company serves enterprise and mid-market customers primarily in North America, the UK and the EU, and has been adopted by leading banking, insurance, financial services and healthcare organizations, among others. Headquartered in New York and Israel, with offices around the world, Panorays is funded by numerous international investors, including Aleph VC, Oak HC/FT, Greenfield Partners, BlueRed Partners (Singapore), StepStone Group, Moneta VC, Imperva Co-Founder Amichai Shulman and former CEO of Palo Alto Networks Lane Bess. Visit us at **www.panorays.com**

For more information: info@panorays.com