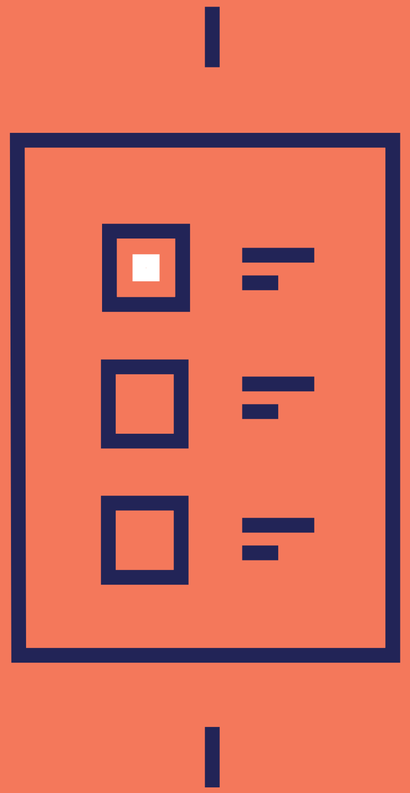
Panorays

10 More Key Questions to Include in Your Vendor Security Questionnaires



Third-party security risk management is more critical than ever.

The number of vendors we work with to enable our businesses continues to grow. Cyberattacks such as SolarWinds, Kaseya and Accellion are more frequent, more sophisticated, more costly and more damaging. In fact, according to recent Kaspersky research, third-party incidents became the most costly enterprise data breach of 2021.

Cybercriminals will continue to take advantage of suppliers as a means to gain easy access to companies. Not only do smaller vendors, partners and suppliers often have more lax security than larger companies, but the ability to strike multiple victims is appealing to hackers.

For these reasons, companies must carefully check their vendors' cyber posture, and the initial vetting of any third party typically begins with a comprehensive security questionnaire. But these are often extremely challenging for cybersecurity professionals because security questionnaires often include hundreds of questions, many of which are irrelevant to organizations. Companies would like to ask fewer questions but are unsure which are critical to include in a questionnaire.

Following the great success of our first guide on "10 Key Questions to Include in Your Vendor Security Questionnaire," we offer 10 more questions that you should be sure to ask your vendors before conducting business with them.

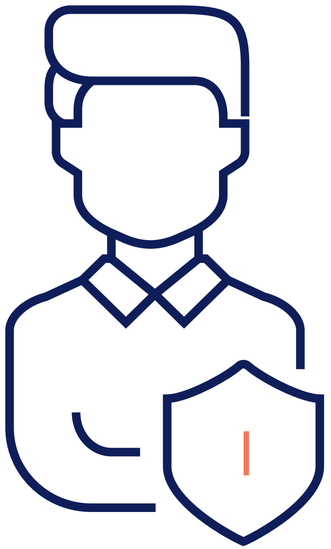
Panorays

01

Does the vendor have a CISO or other information security professional developing and implementing an Information Security Management Program?

Why it's important

Because data is one of an organization's most important assets, you must prioritize its security. To do so, a C-level executive should be charged with the responsibility of protecting digital information by implementing an Information Security Management Program, a control framework based on the CIA (Confidentiality, Integrity, Availability) Triad, the foundation in the development of security policies designed to protect data.



Panorays

02

Does the vendor have a documented third-party security risk management policy and corresponding program in place to manage the risk assessment, selection, oversight of subcontractors e.g., service providers, dependent service providers, sub-processors?

Why it's important

Your vendor's third parties—otherwise known as your fourth parties—increase your attack surface for potential cyberattacks. The more third and fourth parties you are connected to, the more potential vulnerabilities and cyber risk you could face. This document establishes your vendor's official third-party security risk management policy for its organization and for all its vendors and subcontractors, thus substantiating fourth-party security for your organization.

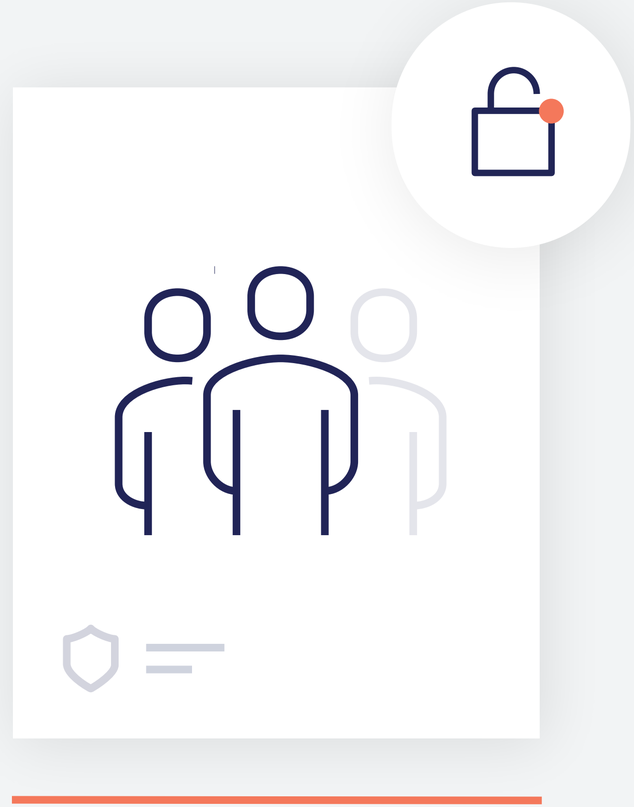
Panorays

03

Does the vendor train employees about phishing risks on a regular basis?

Why it's important

Phishing, a social engineering attack, is when a cybercriminal sends a fraudulent message that appears real and is designed to trick employees into revealing sensitive information or to deploy malicious software on the victim's infrastructure. If a vendor suffers a phishing attack, that could leave you vulnerable as well. Studies show that if you don't repeat security training for employees, their ability to defend themselves against phishing attacks decreases. With phishing attacks on the rise, be sure to prioritize this issue as part of your vendor's security training.



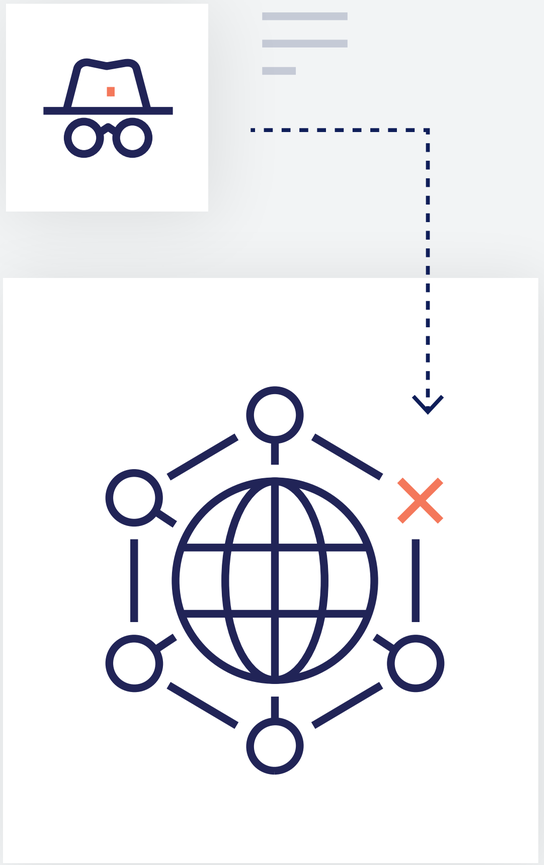
Panorays

04

Does the vendor have a Business Continuity Plan?

Why it's important

A Business Continuity Plan is a proactive plan to avoid disruption of operations and mitigate resulting problems if and when an event such as a cyberattack occurs. Be sure that your vendor has a Business Continuity Plan in place so that if something happens to your vendor, there is a contingency plan in place so it won't impact your business. This shows you that your vendor is a reliable partner that considers its customers and partners.



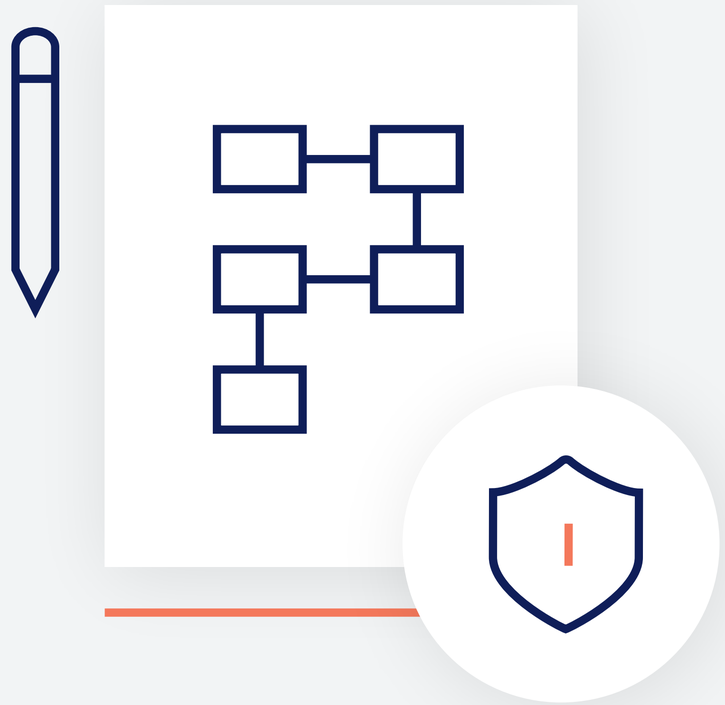
Panorays

05

Does the vendor have an established Business Resiliency Program that has been approved by management, communicated to appropriate constituents and has an owner to maintain and review the program?

Why it's important

A Business Resiliency Program is broader and more strategic than a Business Continuity Plan. While a Business Continuity Plan is a proactive plan to avoid and mitigate risks associated with the disruption of operations, a Business Resiliency Plan is used to anticipate potential disruptions and adjust accordingly. An organization with a Business Resiliency Program doesn't just check a box stating that there is a continuity plan in place, but that it is vigilant about considering current events and making necessary adjustments to better weather whatever storm may come its way. The better your vendor plans, the better it is for your business in case of a disruption such as a cyberattack.



Panorays

06

How does the vendor monitor suspected unauthorized access to data?

Why it's important

The earlier your vendor detects an intrusion, the earlier it can respond and prevent further damage, including potential damage to your organization. Unauthorized access to data can result in disclosure of not just your vendor's confidential or sensitive information, but yours as well. It's important for vendors to assess the amount and the critical nature of the data that employees can access. Companies should conduct periodic reviews of users and permissions, modify user access and even make sure to fully erase obsolete laptops before disposal. By limiting access to critical data, your vendors can reduce the threat of an attacker accessing the corporate network, which of course can trickle down to accessing your organization's private data.

Panorays

07

How soon will the vendor notify you in case of a breach or suspected security incident?

Why it's important

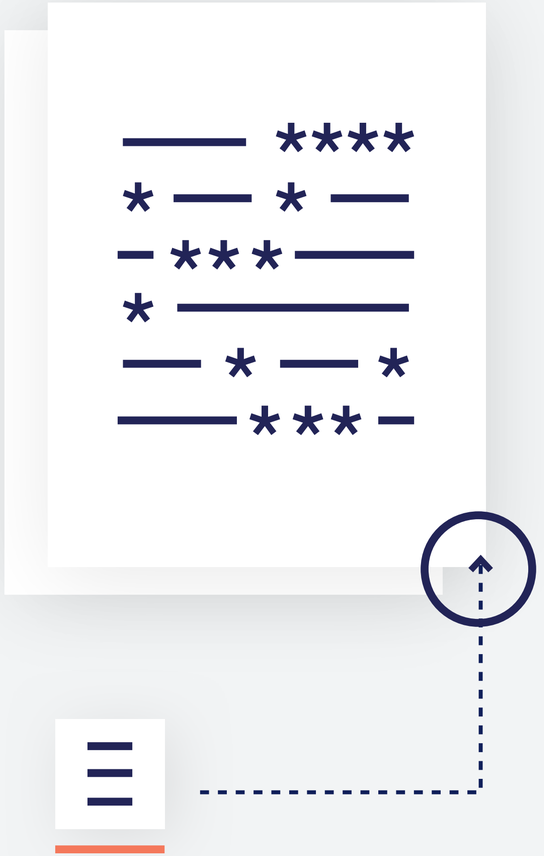
The best way to minimize damage is to be alerted of a breach as soon as possible. This enables you to quickly and methodically conduct all necessary investigations regarding any potential damage caused by the cyberattack on your third party. It's important to note that some regulations, such as GDPR and HIPAA, for example, require companies to notify a supervisory authority of a cyber breach within a specific period of time. Of course, in addition, you may also be required to alert your customers as well.

Panorays

Does the vendor encrypt data at rest and data in transit?

Why it's important

Encrypting data makes it much harder for a hacker to use stolen data. One of the most effective data protection methods for both data at rest and data in transit is data encryption. When data is at rest and stored in a laptop, for example, it's at risk of theft. However, even if criminals manage to break into the device, most likely they won't be able to utilize the data if encrypted. To protect data at rest, you can simply encrypt sensitive files prior to storing them and/or choose to encrypt the storage drive itself. Data in transit is data which is actively moving from one location to another, such as through a private network or across the internet. Companies often choose to encrypt sensitive data prior to moving and/or use encrypted connections (HTTPS, SSL, TLS, FTPS, etc.) to protect the contents of data in transit.



09

Is the vendor prepared to comply with data privacy regulations that you are subject to?

Why it's important

Consumers need to trust that their personal data will be handled with care and that the organizations entrusted with this private information will take that responsibility seriously. A lot of private data is stored online and in company databases, so a data breach can have huge ramifications for consumers as well as for the businesses charged with protecting their data. It is no wonder that data privacy has taken center stage over the past few years with regulations such as GDPR and CCPA. Unquestionably, there will be more to follow. In order for suppliers to work with you, performing the necessary steps to comply with data privacy regulations is non-negotiable and a prerequisite for working together.

Panorays

What measures has the vendor implemented to adjust for remote and hybrid work?

Why it's important

The sudden transition from in-company to remote working presented a wave of cybersecurity challenges in March 2020 at the onset of the COVID-19 pandemic. Security teams needed to address issues such as lack of strategic support, employees connecting via their own devices and fending off increased phishing attacks. On top of this, the same concerns rippled through the supply chain, where vendors were facing the same security challenges. What's clear is that remote and hybrid work are going to be with us for some time—perhaps forever for some organizations. Your suppliers need to show that they have created strategic security processes and procedures, considered technology risks and take the responsibility of vendor security seriously.

Summing Up

These, and the previous 10 questions, are just some of the security issues that should be addressed with your vendors. To ensure a strong cyber posture, companies must fully investigate their vendors' security policies—and automation can help significantly.

Using Panorays' automated, easy-to-customize security questionnaires, you include only the questions that are relevant for each supplier (in the language they require), and can easily track progress. You can choose from a built-in template or create your own.

With Panorays' Smart Questionnaires™, organizations can:

Increase efficiency and effectiveness by eliminating the tedium and delay of manual questionnaires

Get answers faster (as soon as 8 days) and onboard vendors more quickly.

Be assured your suppliers are in alignment with your company's security policies, regulations and risk appetite.

How Panorays Can Help

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.

Unlike other solution providers, Panorays combines automated, dynamic security questionnaires with external attack surface assessments and business context to provide organizations with a rapid, accurate view of supplier cyber risk. It is the only such 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 a company's security policies and risk appetite.

Panorays is a SaaS-based platform, with no installation needed, and is the missing link that creates an out-of-the-box process and security plan, which also easily integrates into existing organizational workflows and systems. It is trusted by organizations worldwide in industries such as financial services, banking, insurance and healthcare, among others.

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

Panorays

Want to learn more about how Panorays' automated questionnaires can help your third-party security process?
Request a demo today!