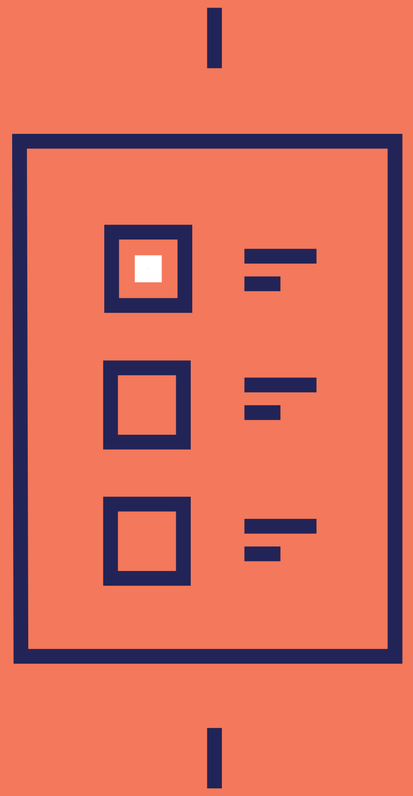
10 Critical Issues to Cover in Your Vendor Security Questionnaires

Panorays



In today's perilous cyber world, it's crucial for companies to assess and monitor the security of their vendors, suppliers and business partners. Failing to do so can be risky, because hackers frequently steal sensitive enterprise data by targeting the third parties to which enterprises are connected. In addition, regulations like GDPR and NYDFS are holding businesses accountable for their third parties' cybersecurity and enforce stiff penalties for those that don't comply.

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 can be a headache, because many questionnaires include hundreds of questions, and many of them are irrelevant. A lot of companies would prefer to ask less questions, but don't know what are the critical questions they have to ask.

What are some of the matters that should be addressed to determine if vendors have a strong cyber posture? Here are 10 important questions you should never forget to ask:

Panorays

01

Does customer data leave the vendor's production systems under any circumstances?

Why it's important

Various data privacy regulations such as GDPR and CCPA require companies to be able to rapidly track customer data. Any customer data that leaves a vendor's realm can be highly problematic since it's not easily trackable.

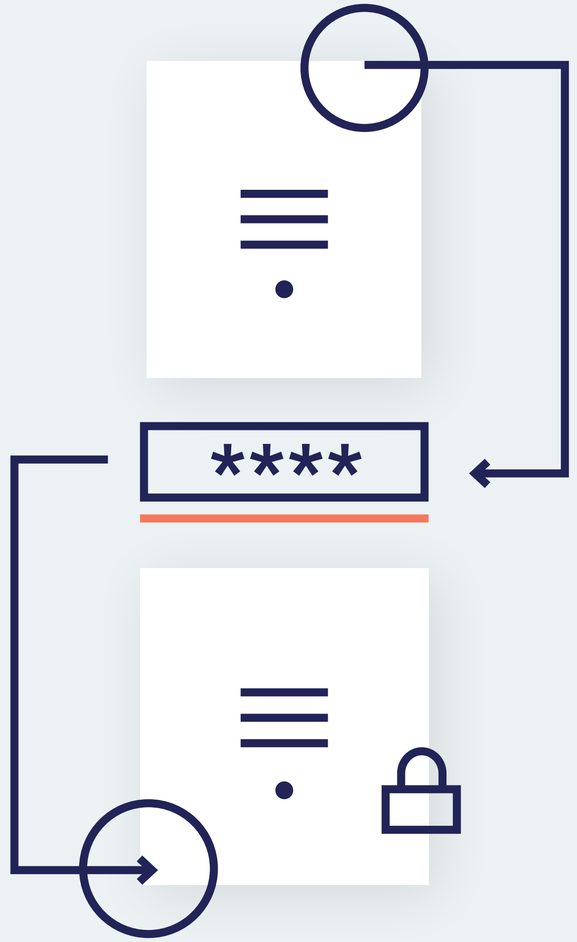
Panorays

02

Does the vendor support single sign-on for internal systems and customer access?

Why it's important

From a security perspective, it's always preferable for companies to use single sign-on. Using single sign-on reduces risk because users are less likely to write passwords down, repeat passwords or create simple or commonly used passwords. It also ensures that employees use correct company authentication standards. As a result, strong password policies are better enforced.



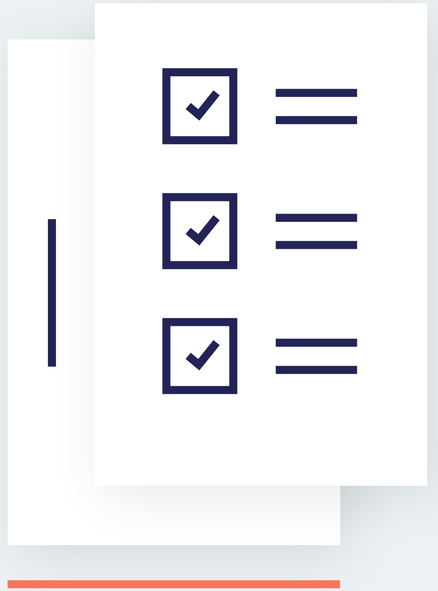
Panorays

03

Does the vendor comply with policies and/or regulations such as SOC2, GDPR, CCPA, NIST, COBIT and ISO-27001/2?

Why it's important

Data security and privacy regulations require companies to put processes in place to protect customer data. In many cases, companies that work with vendors are responsible for the vendors' compliance as well. Knowing that vendors adhere to these requirements is an important part of evaluating cyber posture and demonstrating due diligence.



Learn more > Is CCPA the new GDPR?

Panorays

04

Do the vendor's employees access data on a "need to know" (privileged access) basis?

Why it's important

Unfortunately, many companies grant employees access to company data that they probably should not be permitted to see. Because more people have access to sensitive data, hackers have more opportunities to target employees to steal information. Restricting access to sensitive data results in reducing a company's attack surface. For this reason, it's important for companies to limit employee access to data.

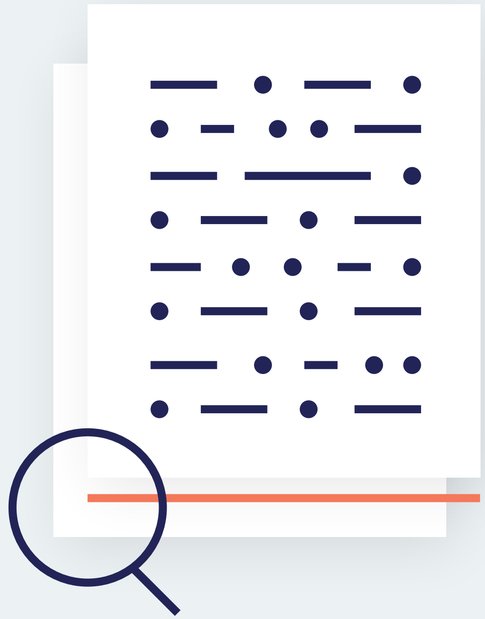
Panorays

05

What processes does the supplier implement to identify possible misconduct?

Why it's important

It's crucial for the vendor to have processes in place to flag whether someone has unauthorized access to systems. Monitoring and alerting systems like SIEM software are particularly useful for this purpose.



Panorays

06

Does the vendor have an employee security awareness program?

Why it's important

Most cyberattacks involve some sort of human targeted attack as well, including social engineering, stolen credentials and phishing campaigns. For this reason, it's important to train employees to protect confidentiality. A security awareness training program addresses this need by educating employees about data management, safe internet habits, social networking dangers and more.

Learn more > Employee attack likelihood: The hidden indicator nobody talks about

Panorays

07

Does the vendor allow Wi-Fi access to internal networks? If so, how does the vendor secure it?

Why it's important

Unrestricted Wi-Fi access can pose a security risk, because users might accidentally download a malicious program or connect an infected device to the network. It's highly preferable to use WPA2 for wireless security, which has strong encryption and is considered significantly more secure than WPA and WEP. If the vendor does allow Wi-Fi access but uses WEP or WPA, that's a clear indication that something is amiss with their security measures.

Panorays

08

Are the vendor's servers hardened?

Why it's important

Server hardening is the process of enhancing server security, which results in a much more secure server operating environment. Since the vast majority of computing resources are online, server hardening is a must to ensure a strong cyber posture.

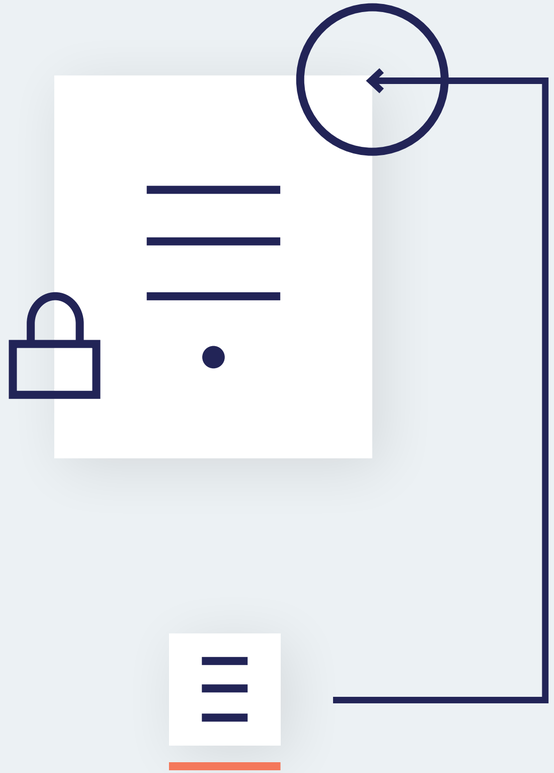
Panorays

09

Does the vendor have controls in place to prevent unauthorized access to its application, program or object source code to ensure it is restricted to authorized personnel only?

Why it's important

Similar to privileged access, this question addresses the issue of limiting unauthorized access to systems by implementing controls such as password protection, two-factor authentication and firewalls. Access control security helps ensure that data is only viewed by people who are permitted to see it.



Learn more > Elements that third-party risk assessments miss

Panorays

10

Does the vendor store sensitive data encrypted in the system?

Why it's important

Because vast amounts of personal information is managed online and stored in the cloud, any sensitive data should preferably be encrypted so that it cannot be read by anyone without authorization. In addition, regulations such as GDPR and CCPA strongly recommend that companies encrypt sensitive customer data. For these reasons, encrypting data is a key step for keeping data secure.

Panorays

Summing Up

These 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. You can create questionnaires using spreadsheets and other manual processes or by using automated systems like Panorays.

About Panorays

Panorays automates third-party security lifecycle management. With the Panorays platform, companies dramatically speed up their third-party security evaluation process and gain continuous visibility while ensuring compliance to regulations such as GDPR and NYDFS. It is the only platform that enables companies to easily view, manage and engage on the security posture of their third parties, vendors, suppliers and business partners. Panorays is a SaaS-based platform, with no installation needed.

Panorays

Want to learn more about how Panorays can strengthen your cyber resilience?
Contact your Panorays sales rep or email us at info@panorays.com