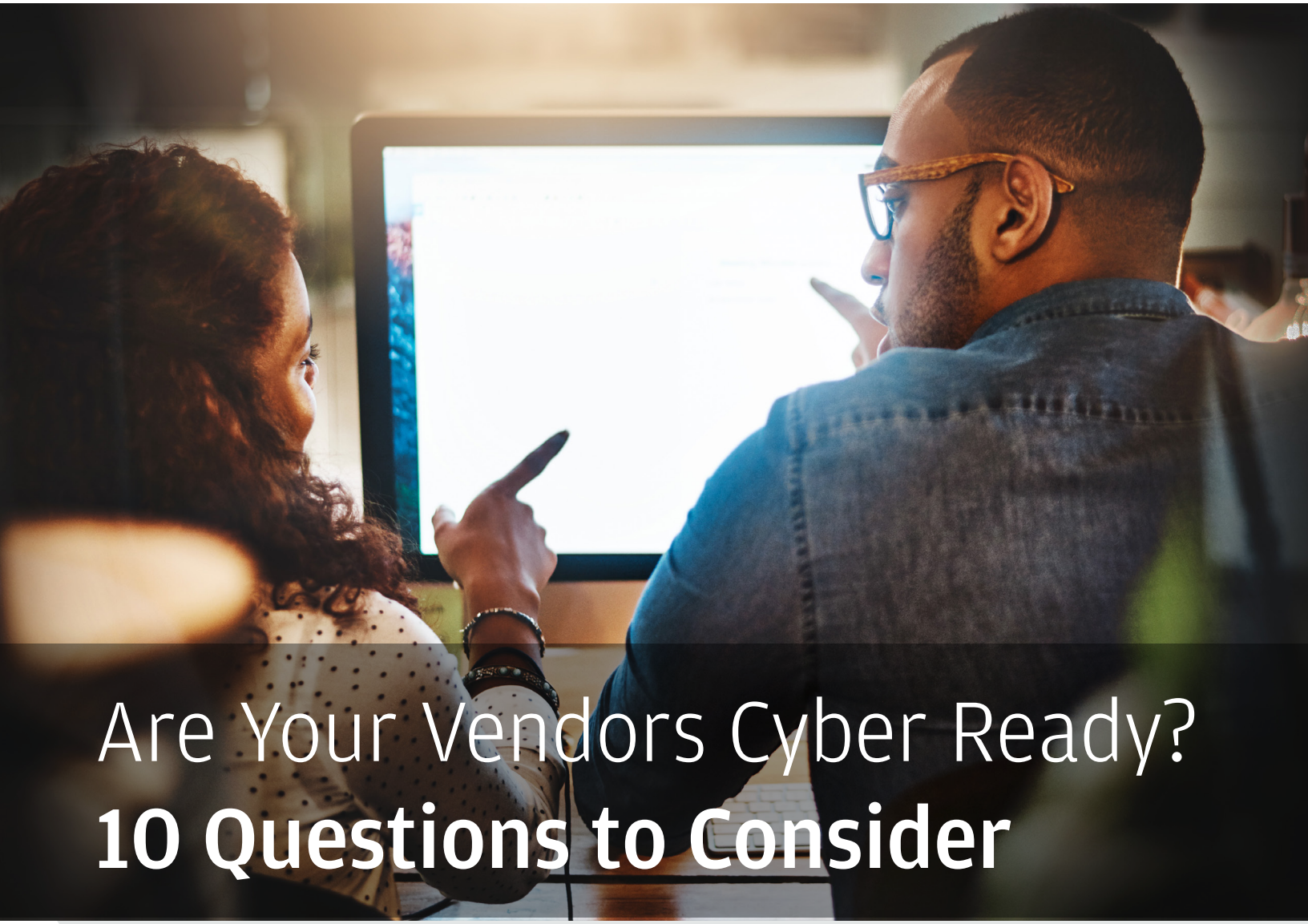

Are Your Vendors Cyber Ready? **10 Questions to Consider**

Even if your organization isn't directly targeted by a cyber incident, you could still feel the impacts of a supply chain attack. Here are 10 questions to consider asking your third-party vendors about their risk assessment.

continued on next page >

The widespread fallout from the supply chain attack on the information technology firm SolarWinds serves as a reminder that businesses must remain vigilant in scrutinizing the risks associated with their third-party vendors. Even if your business is not directly targeted by a supply chain attack, it could still suffer financial loss and other impacts stemming from an attack on one of your vendors.

"In a supply chain attack, criminals use your trusted vendors as gateways to gain access to your organization," said Jim Connell, Head of Global Supplier Services and Chief Procurement Officer with JPMorgan Chase & Co. "Hackers look for vulnerabilities within your vendor's network systems or manipulating the code in third-party software that are interconnected to your organization. Once cybercriminals breach those systems or applications, they can access your network."

As organizations heighten oversight and expand vendor due diligence protocols, they will need to address additional cybersecurity risks with software platforms and network systems. These considerations range from evaluating vendor preparedness to utilizing a third-party risk management service. One example, TruSight™, was founded in part by JPMorgan Chase & Co. and is designed to assess compliance by financial services industry suppliers with rigorous compliance and regulatory requirements.[1] Following a thorough evaluation and review process, TruSight scrutinizes each supplier's security practices and shares an assessment with multiple financial institutions.

Organizations should have an existing set of internal cyber controls and review existing vendor due diligence programs to ensure that they maintain your policies and procedures. If your organization doesn't have a third-party risk management program, now is the time to establish safeguards to help protect employee and client data.

What Should You Protect?

What needs to be protected varies based on your supplier relationship and the services they provide. For example, before JPMorgan Chase exchanges data with a third-party supplier, we assess their security and control environments to ensure suppliers do not introduce any unnecessary or unacceptable risk to our network.

What Is Your Liability If a Vendor Is Breached?

Liability varies based on relationship. However, if a supplier processes, stores or has access to your data, you are ultimately responsible for protecting that information. If data you own is exposed when one of your suppliers is impacted by a data breach, your organization could suffer reputational and financial impact. To address these risks in your operations, identify liability impacts and specify responsibility in your vendor contracts to protect assets and stipulate when you are alerted if a breach occurs.

Top 10 Vendor Cybersecurity Questions to Ask

Vendor risk management should look at four categories: governance, network architecture, security hygiene and incident response. Here are 10 examples of strong vendor management questions you should consider asking your suppliers to mitigate risks to your network systems:

GOVERNANCE

1. Does your vendor have a documented set of rules and procedures regulating the use of information?
2. Does your vendor have established policies and procedures for making changes to its own business processes, systems, networks and applications?

[1] TruSight's services are subject to its applicable service terms.

continued on next page >

ARCHITECTURE

3. Are there robust controls throughout your vendor's network infrastructure to help safeguard data and control access to network systems?
4. Does your vendor use encryption during the storage and transmission of sensitive data, and do they adequately protect encryption keys?
5. Is access to systems, applications and data monitored, logged and restricted to only authorized individuals with the minimal level of access necessary to complete job functions?

SECURITY HYGIENE

6. Is there a documented assessment process to identify, evaluate and report security vulnerabilities in your vendor's network, systems or applications?
7. Are there controls to detect, prevent and alert in the event of network intrusion, either as insider threats or cybercriminals?
8. Will your vendor ensure that it will keep information systems' security configurations and security patches up to date, and will they provide documentation to confirm?

INCIDENT RESPONSE

9. Is there a documented incident response plan specifically for cybersecurity and data breaches, and does the vendor periodically test it for effectiveness?
10. Can the vendor ensure timely and orderly recovery of business, support processes, operations and technology components within an agreed-upon time frame following an incident?

At a high level, there are varying courses of action to take if a vendor answers no to any of the above questions:

- For new suppliers, make sure to note in the contract that your business relationship is contingent upon remediation of high-risk control gaps. Also, consider suspending data sharing with the vendor until gaps are addressed.
- For existing suppliers, based on the severity of the gap, your organization should create an action plan that sets a timeline for remediation based on the level of risk. That includes monitoring the supplier's progress toward satisfactory performance in controls.

Above all, if a supplier is unwilling to provide information about their control environment or remediate weaknesses in it, it's probably best to find an alternate provider. Suppliers should care as much about their clients' security as their own.

Overall, trust but verify that your vendors are keeping systems secure. And if gaps are found, ensure that they are escalated and addressed quickly to protect both your business and your suppliers.

Key Takeaways

- Hackers launch supply chain attacks by identifying vulnerabilities in your vendor's computer networks or software programs to launch a cyberattack against your organization.
- Conduct a strict due diligence review of your vendor's cybersecurity protocols and require any gaps to be fixed.
- Identify liability and specify responsibility in vendor contracts if a data breach occurs.

TIP: JPMorgan Chase publishes our supplier minimum control requirements guidelines, which may be helpful to your organization when considering your vendor preparedness.

The previous article is an excerpt from Fraud + Cybersecurity Magazine: Summer 2021.

Explore the full issue