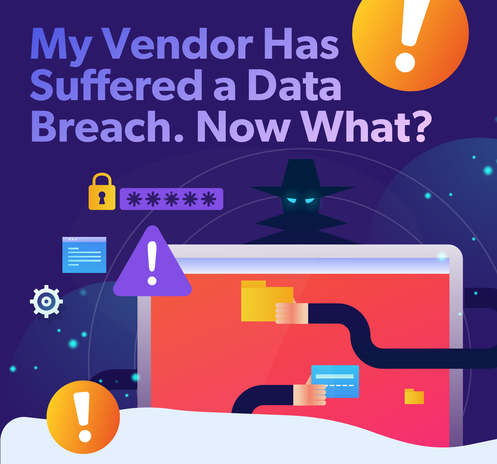
My Vendor Has Suffered a Data Breach. Now What?



Third-party data breaches are occurring more frequently, costing companies time, money, and reputation damage. Threat actors often target third-party vendors because it lets them gain access to and disrupt for profit multiple organizations at once. When a vendor has a data breach, it's challenging to navigate the aftermath while maintaining a positive working relationship.

Follow this step-by-step guide for actions to take immediately after a vendor data breach and tips to mitigate the damage. These steps ensure a quick and effective response while protecting your organization and maintaining customer trust.

Immediate Steps to Take After a Vendor Data Breach

Once you discover a vendor data breach, act quickly to mitigate the potential damage to your organization. Here are seven initial steps to take:

1. **Determine the impact** – Reach out to the vendor to understand the extent of the breach and if your organization's information was impacted. The vendor may not know the full impact yet, so follow up with the vendor on an ongoing basis.
2. **Review your incident response plan** – Your incident response plan includes details specific to your organization for a vendor data breach such as customer services and associated business processes impacted. Review the plan to ensure both you and the vendor are taking the correct steps.
3. **Contact your cyber insurance carrier** – Your cyber insurance carrier will have specific requirements for notification associated with filing claims. Inform them as soon as possible as they may require using their incident response process and associated cyber forensic teams where required.
4. **Inform your regulators** – Know your requirements. Several regulatory agencies and state governments, including the Securities and Exchange Commission (SEC), have stringent data breach notification requirements. For instance, FDIC supervised banking organizations require notification no later than 36 hours, while federally insured credit unions must notify the NCUA no later than 72 hours. Once you've confirmed your information was compromised, notify your regulators.
5. **Secure your systems** – Depending on the impact, immediately isolate any affected systems and take them offline. Change access credentials to prevent further data loss and implement your manual workaround procedures until systems are deemed safe and accessible.
6. **Notify your customers** – Be transparent with your customers or members and notify any impacted individuals. Inform them about the breach and the steps being taken by your organization and the vendor.
7. **Offer support services** – This generally includes free credit monitoring or identity theft protection to affected individuals. If customers have access to compromised online tools, update user authentication procedures to be more robust, like multi-factor authentication.

Steps to Take After the Immediate Impact

Once the dust settles and your organization has secured its data, there are still steps to follow to further protect your organization.

Review lessons learned – Perform a security assessment to learn what worked and what didn't. The assessment may also reveal overlooked security gaps.

Revise the incident response plan – If changes are needed, be sure to note them in the incident response plan and discuss them with the vendor.

Re-evaluate the vendor relationship – Review the vendor's security practices and ask what changes they're implementing post-breach. Review and update the vendor contract for stronger security provisions if needed. Although you may choose to continue the vendor relationship, it's still important to assess the vendor's response.

Refresh employee training – It's always wise to refresh employee and vendor security training after a breach. Most data breaches originate from human error, so reminding employees and vendor employees of best practices can help prevent future breaches.

Tips to Mitigate Vendor Data Breaches

Although your organization can't fully prevent a vendor data breach, there are still best practices to mitigate the damage.

Be transparent – Be transparent with your customers and stakeholders. This will go a long way to regaining trust. Communicate with stakeholders about everything your organization is doing to protect data.

Include data security protections in the vendor contract – Review vendor contracts and templates to ensure data security protections are included. This includes data breach notifications, encryption requirements, and the right to audit vendor security documents.

Continuously monitor vendor security – A vendor's security posture can change at any moment. Monitor the vendor's security environment consistently through risk intelligence so you can act quickly when an issue occurs.

Prioritize cross-collaboration – Your organization can have a quicker response when it works collaboratively across departments and with the vendor. Consider who needs to be involved, like Legal, InfoSec/Cybersecurity, Marketing, etc. Document this in your incident response plan.

Encrypt sensitive data – Data encryption should be a regular practice at your organization and with your vendors. Encrypt all sensitive data shared with vendors both in transit and at rest. Regularly update encryption keys.

Limit vendor data access – Practice the principle of least privilege and only share what's necessary with your vendors. Separate vendor access from your main network to minimize potential impact.

Conduct exercises – Conduct exercises which consider if the services of critical vendors are disrupted due to a cyberattack on the vendor. This will prepare your organization by practicing manual workarounds when vendor systems are compromised. Consider including your vendor in exercise conversations and ask them how their incident response impacts your planning so you can close any gaps in expectation.

A vendor data breach can impact your organization at any time. A quick and proactive response can minimize the damage and save your organization's reputation. Following security best practices lowers the risk of destructive vendor data breaches.