PUTTING BLIND TRUST IN YOUR THIRD-PARTY VENDORS?

Help prevent the backlash of a vendor's cyberattack with these key questions.

Today, the chances for an organization to suffer a data breach are high - particularly through third-party vendors. According to a recent SecureLink/Ponemon Institute study:

59% of respondents said their organizations had experienced a data breach caused by one of their third-party vendors.

36% of organizations evaluate a vendor's security practices before they start sharing sensitive information with them.

Because the liability for keeping that confidential data private lies with whoever the data was entrusted with in the first place, organizations that don't thoroughly vet vendors can be particularly vulnerable.

For example, if a payroll vendor suffers a data breach, the company that was originally entrusted with the employee data remains liable for any resulting damages.

If your organization outsources business functions like IT, HR, accounting, or payment services, it's important to keep the sensitive data shared with them – names, addresses, salaries, bank account or credit card numbers – as secure as possible.

How can you be sure that your vendors take cyber security as seriously as you do? And how can you vet them so you're confident that they're using the latest and greatest best practices to protect your data once it's out in the ether sphere?

ASK THIRD-PARTY VENDORS AND SERVICE PROVIDERS THESE QUESTIONS:

AHT
INSURANCE
A BALDWIN RISK PARTNER

1 WHAT ARE YOUR BACKUP PROCEDURES?

Find out if there's ability to recoup data quickly if an incident (e.g. ransomware) occurs. *Look for:*

- Redundancy in both online and offline data
- Files stored in a physical server somewhere and in a separate account in the cloud
- Regular testing of backup systems so you know they're working

2 WHAT CYBER SECURITY REGULATIONS ARE YOU IN COMPLIANCE WITH?

If you share personally identifiable information, financial data, and personal health information with a vendor, you want to make sure that the security practices it uses can instill a high level of trust in your employees and customers who provided the information. Being confident that a vendor's security measures can strengthen (not compromise) the overall security posture of your own organization is critical. *Look for:*

Compliance with:

- Federal laws under **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** if you will be sharing medical or health data with vendor
- Rules set by the **Payment Card Industry Digital Security Standard (PCI DSS)** if you work with a payment tech provider that accepts or stores credit card information from your employees or clients
- **General Data Protection Regulation (GDPR)**, which oversees keeping personal data safe by requiring robust processes for handling and storing personal information
- **Mandatory regulations** for sensitive financial data with a vendor, like bank account information

3 WHAT TYPE OF CYBER SECURITY TRAINING DO YOU PROVIDE FOR EMPLOYEES?

Since 82% of data breaches involve a human error, making sure vendors conduct robust and ongoing security training with employees is critical. *Look for:*

- A culture of training that keeps cyber security top of mind throughout organization
- A written cyber security policy that's reinforced by an employee training program
- Drills and testing that 1) ensure the people who need it most, get it; and 2) limit vulnerability in your organization
- Timely communication about the latest scams
- Consequences if an employee causes a breach

4 WHAT FRAUD PREVENTION TECHNIQUES DO YOU USE?

For companies that work with financial institutions, understand what type of fraud controls the vendor follows, particularly when it comes to wiring money or transferring funds. *Look for:*

- Proof of documented fraud prevention practices
- Comprehensive protocols that generally include: segregation of duties and functions among employees, required signatures for authorizing documents, use of passwords and PINs, dual controls for approving transfers or transactions over a certain amount, forms matching to flag false or unauthorized documents, audits and surveillance of key activities.
- Use of intrusion detection software

5 WHAT TYPE OF RECORD-RETENTION POLICIES DO YOU FOLLOW?

If your organization does business with the European Union (EU), you want to make sure vendors follow standards set by the General Data Protection Regulations (GDPR). As part of your due diligence, find out how they handle and store private data. *Look for:*

- Practices that support the “right to be forgotten”
- How often they purge personal data files
- What secure methods they use to destroy private data so it can’t be recovered once it reaches its “expiration” date or is no longer needed.

6 DO YOU HAVE CYBER INSURANCE AND TECHNOLOGY E&O COVERAGE?

Even if one of your third-party vendors causes a data breach, you want to make sure it has the resources to respond effectively, quickly remedy the situation, and limit damage. (Of course, it’s a good idea for your organization to have coverage, as well.) *Look for:*

Proof of cyber insurance and technology E&O (if they provide services like electronic record-keeping systems) that can help pay for costs after a breach. **For example:**

- Legal help to deal with the aftermath of a breach
- Informing those whose private information was stolen or accessed
- Lost business income due to down systems
- Compliance with regulatory investigations
- Lawsuits and fines related to lack of privacy and security

Of course, assessing vendors for security measures is only one way to address cyber risk. **Connect with us** to discuss all aspects of your cyber security risk strategy... and better position your business to survive a data breach.

Contact Us

This material has been prepared for informational purposes only. BRP Group, Inc. and its affiliates, do not provide tax, legal or accounting advice. Please consult with your own tax, legal or accounting professionals before engaging in any transaction.

AHT INSURANCE
A BALDWIN RISK PARTNER