Breach Risk Prevention Checklist

☑ 1. Conduct Annual Risk Assessments
Security risk assessments can identify areas where your system is strong and where it's weak so you can take appropriate action to resolve any open issues. The risk assessment look at your entire tech infrastructure including data storage, remote access, and documented policies and procedures.

☑ 2. Back-up and Encrypt Data
Having data in only one location is risky because hard drives and storage drives go bad without warning. Whether you choose to back-up and store your data on-site or in the cloud, it should be encrypted to protect the data from being improperly accessed.

☑ 3. Control Access to Sensitive Data
Strict data access guidelines should be in place to manage customer information, critical business files and company systems. A general guideline for many businesses is that users only have access to data and systems that are essential to perform their assigned job responsibilities.

☑ 4. Update Software and Licenses
It's imperative that you keep your security software license current, and software updated with the most current release to repair security holes or fix bugs. This minimizes weak spots that hackers can manipulate. Never hit the "Remind Me Later" button for updating security software.

☑ 5. Update Policies and Procedures
Don't overlook the importance that employees play in protecting company data. Training employees on possible security threats, and actions to take if a security threat is identified can help prevent mistakes that may lead to a data breach of customer and company data.

☑ 6. Monitor In-Network Activity
Data breaches can happen internally as well. With more employees working remotely, it is important for companies to have strong authentication, preferably two-factor, and secure connections in place for remote access.

☑ 7. Evaluate Partners and Vendors
If you're sharing data with partners and vendors or if they have access to your systems, you may want to review their security measures. Privacy laws in many states pertain not only to your company but extend to your vendors and partners and third parties that process or store data on the company's behalf.

☑ 8. Create a Security Incident Response Plan
Even though security measures are in place, companies still experience data breaches to their network and equipment either through an intentional or unintentional act. Therefore, companies need to have a response plan in place to quickly address and control the situation.

☑ 9. Reap Benefits of a Managed Security Provider
Even though security measures are in place, companies still experience data breaches to their network and equipment either through an intentional or unintentional act. Therefore, companies need to have a response plan in place to quickly address and control the situation.

VISUAL EDGE IT