Cyber Risks & Liabilities

The Importance of Data Backup and Recovery Plans for Businesses

WINTERS-OLIVER
INSURANCE AGENCY, INC.

Data is crucial for modern business operations, so a solid data backup and recovery plan is essential. A data backup plan involves creating and storing data copies, while a data recovery plan focuses on restoring lost data to minimize downtime. These plans offer benefits such as reducing financial losses, protecting against cyberthreats, enhancing regulatory compliance, preserving customer trust and saving costs.

Here are tips for creating data backup and recovery plans:

- **Identify critical data to backup**. Identify essential data for daily operations or compliance with regulations. Prioritize backup plans for continuity in case of data loss. Assess backup frequency based on importance.
- **Follow the 3-2-1-1-0 backup rule**. Ensure three data copies (in addition to the original) on two different storage types, with one off-site. Keep one backup offline to guard against cyberthreats like ransomware. Regularly test for "zero errors" in backup integrity.
- **Encrypt data and implement access controls**. Encryption safeguards back up data from unauthorized access, providing a crucial layer of security. Restrict access to authorized personnel, ensuring protection from internal and external threats.
- **Conduct regular testing**. Periodically conduct recovery drills to ensure backup systems function as expected and verify the integrity of backed-up data for smooth restoration in case of a disaster.
- **Automate and monitor backup processes**. Automate backups using technology to reduce errors, and ensure reliability through continuous monitoring.
- **Educate and communicate with staff**. Regularly train employees on data backup and recovery. Ensure they understand any procedural changes to stay aligned with the latest protocols.

Contact us today for more information.

Contingent Business Interruption Insurance for Cyber Events

As cyberthreats evolve, businesses face an increased risk of operational disruptions from digital supply chain failures. Cyber business interruption (BI) insurance protects against financial losses from internal technology failures like data breaches or ransomware attacks. For businesses relying on third-party vendors, cyber contingent business interruption (CBI) insurance goes a step further, covering losses from disruptions in third-party technology systems.

Cyber CBI insurance provides crucial financial protection when events like ransomware attacks on vendors or cloud service providers disrupt an organization's operations. While cyber BI insurance focuses on internal system failures, CBI insurance addresses losses caused by failures in the systems of external vendors and service providers. Despite its value, cyber CBI insurance may exclude certain events and third-party providers, such as disruptions caused by internet service providers and basic infrastructure failures. Coverage is generally limited to cyberattacks, often excluding nonmalicious system failures like technical errors or human mistakes.

Cyber CBI policies usually have a waiting period of six to 12 hours before coverage begins. During this time, organizations must cover their own losses. These policies may also include deductibles or retention requirements, meaning businesses will need to absorb some costs before their coverage starts.

The key benefits of cyber CBI insurance include maintaining financial stability amid costly third-party cyber events and safeguarding businesses against digital supply chain threats. This coverage allows organizations to recover more effectively from cyber disruptions impacting their external vendors and service providers.

The Risks of Collecting Biometric Data

Biometric data refers to an individual's unique physical and genetic traits, such as facial geometry, fingerprints, iris scans and voiceprints. Many organizations now collect biometric data to enhance security, personalize marketing and monitor employees. However, this type of data poses significant risks to privacy and security.

Unlike usernames and passwords, biometric data cannot be easily changed if compromised, which makes it particularly vulnerable to misuse or abuse. Cybercriminals can exploit this sensitive data in breaches or ransomware attacks, potentially leading to serious consequences like identity theft and unauthorized access to secure systems. The impact of a cybersecurity incident involving biometric data can extend beyond the initial victim, potentially affecting their relatives. For example, biometric data, like facial recognition or fingerprint patterns, may have similarities among family members, making them more susceptible to targeted fraud. Furthermore, organizations that mishandle biometric data or fail to protect it adequately could suffer severe reputational damage, including loss of public trust, diminished customer loyalty and potential legal consequences.

The regulatory landscape for biometric data collection is rapidly evolving. While there is no overarching U.S. law specific to biometric data, various state and international regulations, such as Illinois' Biometric Information Privacy Act and the EU's General Data Protection Regulation, impose strict guidelines on how this data should be collected, stored, and used. Noncompliance can result in hefty fines and litigation.

To mitigate these risks, organizations should conduct risk assessments, implement robust privacy practices like data minimization, adopt strong technical controls, educate employees and ensure compliance with applicable laws. Additionally, having a cyber incident response plan and securing appropriate insurance coverage is essential to managing potential losses from biometric data breaches. For additional risk management guidance, contact us today.