Courtesy of
Crendon Insurance Brokers Ltd

CYBERRISKS&LIABILITIES_

Managing Cyber Security During a Merger or Acquisition

During a merger or acquisition, company leaders must scrutinise their insurance, finances and future employee needs. Leaders often postpone cyber security concerns at this time, which is unfortunate because this is when company data is at its most vulnerable.

Data transfers must proceed with no complications, or else the companies risk damaging their reputations, losing customers and hurting future sales. Additionally, the companies must meet their legal responsibilities before, during and after the data transfer process.

Use the following checklist to ensure your data transfer proceeds unimpeded:

1. Identify all data assets that need to be transferred.
2. Gather and merge all data standards, policies and processes from employees at both companies.
3. Identify risks that could occur during the transfer.
4. Prior to any transfers, ensure data is backed up.
5. Run background checks on any employee who will be involved in the data transfer process.
6. Craft a business continuity plan to prepare for potential data loss or outages during the period when the transfer will be occurring.
7. Assign a high-level person the job of overseeing all data transfers. He or she will have the task of assigning one person to each data asset that needs to be transferred.
8. Legally transfer ownership of data assets as quickly and completely as reasonably possible.
9. Host training sessions on new data standards, policies and processes.
10. Update disaster recovery plans, business continuity plans and emergency plans to include newly acquired data assets.
11. Update the risk profiles for newly acquired assets.

Preparing for Data Transfer
Planning for a data transfer should begin as early in the merger or acquisition process as possible. It is wise to assign one person the task of overseeing all data transfers so that there is little room for miscommunication or error. That person can then delegate smaller tasks, such as identifying data assets, pinpointing potential risks during transfer and making sure the data transfer is in compliance with government and local laws, but the person in charge should be aware of the current status of all tasks at all times. This person should also manage the implementation of the interim business continuity plan so that daily operations are disturbed as little as possible.

Crendon
Insurance
Brokers

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.

Keep in mind that if the acquired company has already completed portions of the data transfer or consolidation tasks, you should review the work to ensure accuracy.

Consider relocating IT employees from the acquired company early so that they can help with the data transfer and risk identification process, as they will be more familiar with their data and systems. Set aside sufficient time to convert any older data for use in newer software.

Finally, ensure that your system configuration records are up to date prior to any data transfers or consolidations. This will help isolate any issues that might occur and allow for an effective fix.

Good Practices for Data Transfer

Even if your company is completely prepared for the data transfer, it is still possible that issues will arise during the process. To help hinder these risks, follow these best practices for data transfer:

- Avoid using any kind of removable media to transfer data from one place to another. If the only method you can use is removable media, then take extreme care to be sure all records are encrypted, especially if they involve personal information.
- If you have any data that is not getting transferred, you should dispose of it safely and completely to ensure it cannot be stolen.
- Do not try to move all data at one time. Set small goals to complete every day or week to prevent an overload on your system or large, messy mistakes.
- Consider halting some of your company's cyber services until all data has been switched over in order to protect the services from being adversely affected by the transfer. Another option would be to run a similar service until data has been transferred.
- Increase protective monitoring systems to prepare for the possibility of a disgruntled employee. Mergers and acquisitions are scary, uncertain times for employees, whose roles are often modified or eliminated to accommodate a new company structure. Update all clearances and access capabilities for employees based on new roles and duties.

Safe and secure data transfer during a merger or acquisition is of utmost importance. Communication is crucial during this time and basic duties and responsibilities should be quickly laid out and assigned to employees before, during and after the transition.

Data transfer is not just about preventing and managing a compromise or interruption to services—you also need to keep your customers' and stakeholders' needs in mind, and take their concerns into consideration. Most importantly, ensure your new and existing clients know that you are keeping their data safe.