Cyber Liability

Brought to you by: Bryson Financial

Managing Cyber Security During a Merger or Acquisition

During a merger or acquisition, insurance policies and finances need to be scrutinized and the future of employees addressed. Cyber security is often put on the back burner, which is unfortunate, because this is a time when company data is at its most vulnerable. Data transfers must proceed without a hitch, or else the companies risk damaging reputation, losing customers and hurting future sales. Additionally, legal responsibilities must be upheld before, during and after the data transfer process.

Use the following checklist to ensure you've covered all of your cyber security bases:

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

Preparing for Data Transfer

Planning for 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, identifying potential risks during transfer and making sure the data transfer complies with federal and state law, 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. 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. Sufficient time should be mapped out to allow any older data to be converted for use in newer software and programs.

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.

Consider the following examples of hidden liability:

- A selling company purchased several other organizations in the past few years, all of which the buyer must now track down, whether they still exist or not, in order to identify all their associated liabilities.
- A selling company has legacy exposures, which are ongoing legal claims that arose against the acquired company many years ago. The buyer must research the past cases and determine possible financial implications as well as their impact on its reputation and the possibility that similar cases could arise in the future.

Good Practices for Data Transfer

Even if your company is completely prepared for the data transfer, it's still possible that issues will arise during the process. Here are some good practices your company can utilize to minimize these risks:

- Try to 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 isn't 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.

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 to take their concerns into consideration. Most importantly, ensure your new and existing clients know that you're keeping their data safe.

For additional cyber risk management guidance and insurance solutions, contact us today.