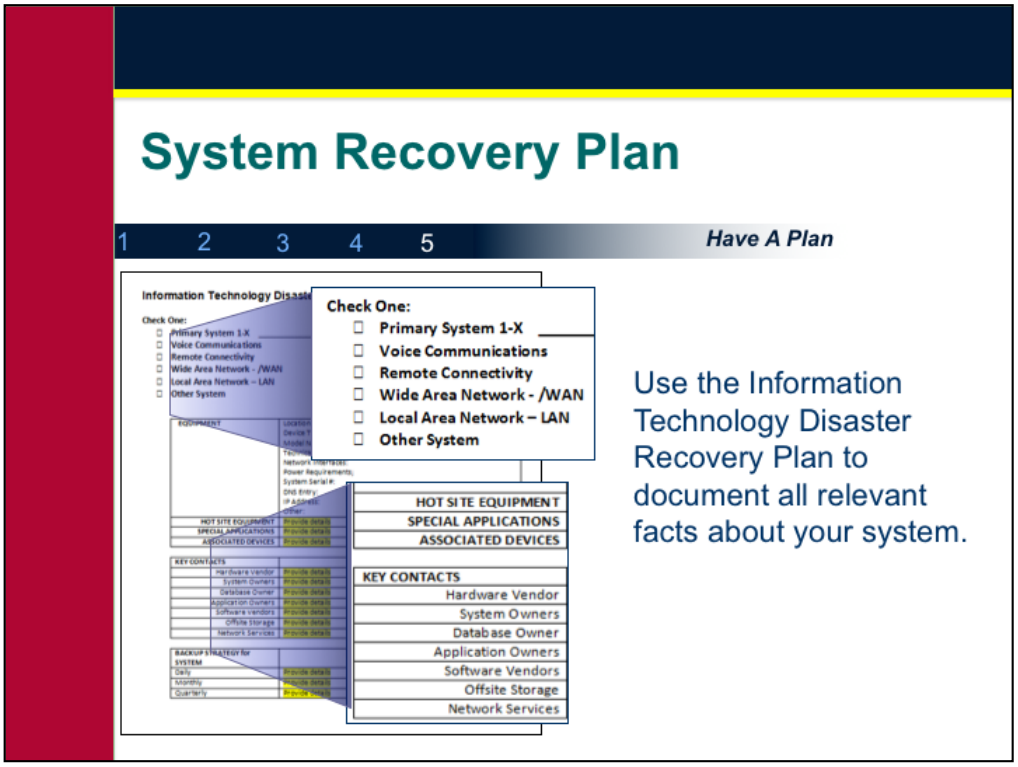
Most businesses use data driven systems and services everyday. Let's look at data security and maintaining continuity of those services.

Organizations can have many combinations of systems to support operations. Disaster recovery planning considers each system separately in order to support total and partial system failures.

Identify all of the types of systems you use to determine how critical they are to business continuation and how systems interrelate and work together. Make sure you identify suppliers for these systems and their Contact Info. Have your account numbers, passwords, and other important information available for each.

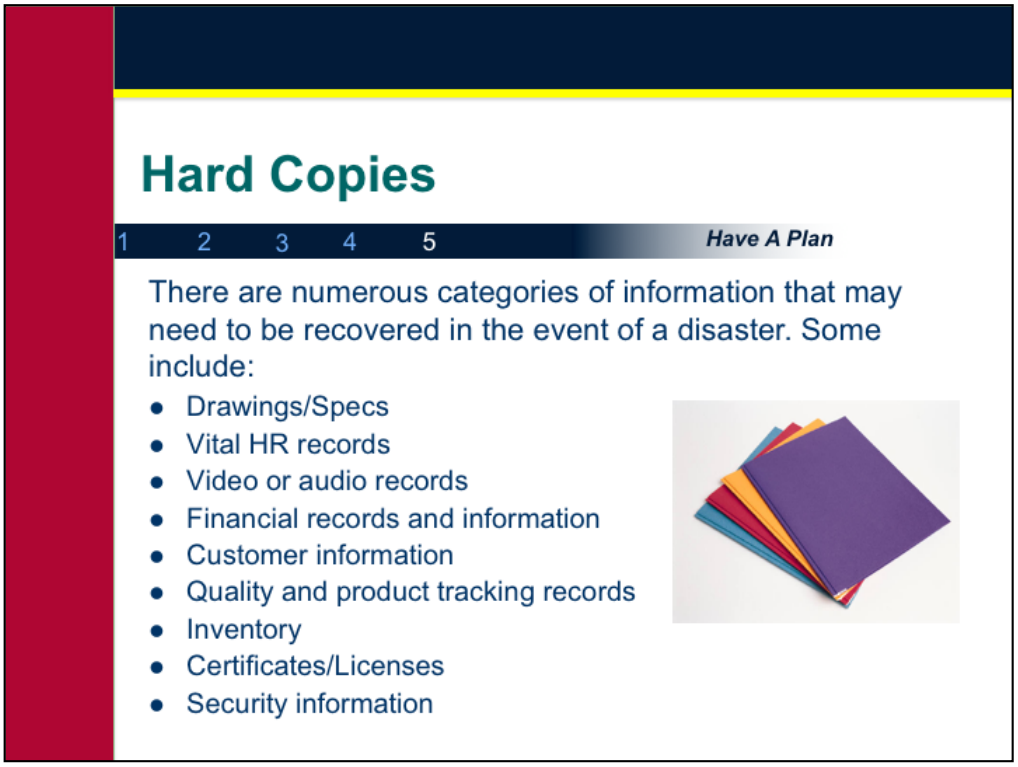
For each system define equipment and support infrastructure. This involves a number of steps, such as:

1. Create an inventory of your equipment – including servers, routers, desktop computers, laptops, mobile phones and other devices.
2. Identity backups to each of these categories – for example, where will you access replacement or redundant server space? How about replacing ruined desktop computers quickly? What if your ability to connect to remote devices is lost?
3. Identify a provider for each of these critical infrastructures – do you have a vendor who will work with you on temporary replacements?
4. Be sure to identify who is in charge of addressing these needs. You can't do everything in a disaster.



Use the Information Technology Disaster Recovery Plan to document all relevant facts about your systems.

KEEP IN MIND: you may update your systems or change your providers – and you'll need to make sure you keep this section up-to-date.



Assess which records and data would be most vital to recover if all was lost forever. How would the organization function without them? What is the safest way to ensure a copy is available if the building and equipment are destroyed? How do you go about recovering this document in the event of a disaster?

Not every record or document is critical. It is ridiculous to address every possible situation. Address the most catastrophic situation that is most likely to occur.

Very few storage systems are 100% disaster proof. Humidity, extreme temperatures, fire, water, and chemicals will destroy or degrade paper, microfilm, microfiche, and aperture cards. Even electronic formats are susceptible to the elements. Duplicates of your vital records should be stored in an off-site location. To minimize damage at the off-site storage, consider the type of destruction possible. For instance, if hurricanes occur in your area, it may be wise to choose a site that would likely be out of harms way should a hurricane destroy your site.

Data and Information Security

1 2 3 4 5 *Have A Plan*

Now that you have an understanding about how to plan for data security data and information availability in your business, download the worksheet Critical Data & Information to begin a new plan for each of your critical systems.