

The slide features a dark blue header with a yellow underline. Below the header, the text 'STEP 5: DATA SECURITY AND AVAILABILITY' is displayed in a dark blue, sans-serif font. A progress bar below the title shows five numbered steps (1-5) in white on a dark blue background, with the text 'Have A Plan' in italics to the right. The number '1' is highlighted. In the center, a grey rounded rectangle with a cloud background contains the text 'Are You Prepared?' in white. A vertical red bar is on the left side of the slide.

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

Systems Approach

1

2

3

4

5

Have A Plan

- Understand system combinations
- Consider each system separately
- Plan for each system in use



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.

System Types

1

2

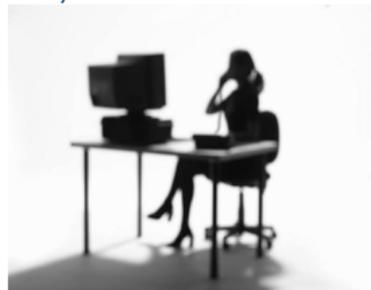
3

4

5

Have A Plan

- Primary System(s) used to directly support operations
- Voice Communications (phone)
- Remote Connectivity
- Wide Area Network - WAN
- Local Area Network – LAN
- Social Media



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.

Planning Approach

1

2

3

4

5

Have A Plan

Create an Information Technology Disaster Recovery Plan for each system

- Equipment
- Key contacts
- Backup process
- Related systems
- Additional contacts



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. Identify 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.

System Recovery Plan

1 2 3 4 5 *Have A Plan*

Information Technology Disaster Recovery Plan

Check One:

- Primary System 1-X _____
- Voice Communications _____
- Remote Connectivity _____
- Wide Area Network - /WAN _____
- Local Area Network - LAN _____
- Other System _____

EQUIPMENT

LOCATION: _____
 DATE: _____
 CHANGE: _____

TECHNICAL SUPPORT: _____
 NETWORK PROVIDER: _____
 POWER REQUIREMENTS: _____
 SYSTEM SERIAL # _____
 ONE KEY OR ADDRESS: _____

HOT SITE EQUIPMENT

SPECIAL APPLICATIONS

ASSOCIATED DEVICES

KEY CONTACTS

Hardware Vendor	Phone: _____
System Owner	Phone: _____
Database Owner	Phone: _____
Application Owner	Phone: _____
Software Vendor	Phone: _____
Offsite Storage	Phone: _____
Network Services	Phone: _____

BACKUP STRATEGY for SYSTEM

DATA: _____
 LOCATION: _____
 QUARTERS: _____

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

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.

Hard Copies

1

2

3

4

5

Have A Plan

There are numerous categories of information that may need to be recovered in the event of a disaster. Some include:

- Drawings/Specs
- Vital HR records
- Video or audio records
- Financial records and information
- Customer information
- Quality and product tracking records
- Inventory
- Certificates/Licenses
- Security information



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.