Data Loss Prevention Questionnaire

Critical Data

What data is your most critical data? (Ex: accounting, customer orders, inventory, payroll, marketing database, taxes, contracts, etc.)

When thinking about your most critical data:

1. How far back in time do you need to be able to restore that data? (Will you ever need to access that data the way it was 1 week ago? 1 month ago? 1 year ago? 3 years ago? 10 years ago? Etc.)

2. How much of your most critical data can you afford to lose? (If a disaster strikes and you lose the last 24 hours of data, is that OK? What about if you lose the last 5 days of data?)

3. Considering your answer to question 2, how much will it cost you to replace that amount of lost critical data? (For example, if you answered 24 hours to question 2, what would it cost you to replace, recreate, or re-enter data from the last 24 hours? Consider how difficult it might be to first determine what data needs to be recreated, then find the information again, re-enter that data, and confirm it's all correct. Will you need to pay overtime or other extra expenses in order to complete the data recovery?)

4. If your critical data is lost, how long can you afford to wait while the data is being restored? (Ex: 3 business days, 1 business day, 4 hours, 1 hour, etc.)

5. Considering your answer to question 4, how much will it cost you to wait while your critical data is being restored? (For example, considering a 3 person accounting department waiting to have data restored before they can work again – the least it would cost you is the total payroll per hour for 4 people (the 3 accounting people plus 1 IT person) multiplied by the number of hours they couldn't do their job while your critical data is being restored. But your real cost would likely also need to include delays in accounts receivables, penalties for late payments of AP, distractions and delays for other staff affected by the situation, having to pay overtime, and more.)

Non-Critical Data

When thinking about the rest of the data (your non-critical data) within your organization:

1. How far back in time do you need to be able to restore this data from?

2. How much of it can you afford to lose? (1 month, 1 week, 1 day, 1 hour, etc.)

3. What will it cost to replace that lost data considering your answer to question 2 above?

4. How long can you afford to wait while this non-critical data is being restored?

5. What will it cost you to wait while the non-critical data is being restored?

Related Questions

1. Do you have a legal obligation to keep any data for a certain time-period? (For example, financial info that affects tax calculations may need to be kept for several years.)

2. Is there any data that would not cause a problem if it was lost? (Temporary files, etc.?) Can this throw-away data be separated from the more important data in a way that makes backup boundaries clear?

3. Are you certain that all your staff are saving their files and data to locations that are being backed up?

    a. How are you certain?

4. How can you be certain that your backup plan is working? Do you periodically test the backups by restoring data to confirm the backup and the restore plan work as expected?

    a. How often do you perform test restores to verify your backups are working as expected?

Backup System Details:

Critical files and data locations (Server, folders, SQL database name, etc.): _____

_____

_____ Critical data retention period (days, weeks, months, years)

_____ Critical data backup interval (minutes, hours, days)

_____ Critical data restoration time (minutes, hours, days)

_____ Cost of potential data loss ($)

_____ Cost of data duration time ($)

Redundant backup solution details (data, backup location, frequency, etc.): _____

_____

Offsite backup solution details (data, backup location, frequency, etc.): _____

_____

Non-critical files and data locations (Server, folders, SQL database name, etc.): _____

_____

_____ Non-critical data retention period (days, weeks, months, years)

_____ Non-critical data backup interval (minutes, hours, days)

_____ Non-critical data restoration time (minutes, hours, days)

_____ Cost of potential data loss ($)

_____ Cost of data restoration time ($)

Verification / guarantee that all data is stored in locations that are backed up: _____

_____

Plan and schedule for performing test restores of backup data: _____

_____

Checklist:

- ☐ Critical data is identified and documented
- ☐ Retention period for critical data meets business requirements
- ☐ Backup frequency (interval) limits data loss window to within business requirements
- ☐ Data restore process restores data within business requirements timeline
- ☐ Cost of potential data loss is within acceptable business limits
- ☐ Cost of restore duration is within acceptable business limits
- ☐ Redundant backups are in place for all data for which permanent loss is unacceptable
- ☐ Offsite backup is in place to protect against physical disaster of primary backup
- ☐ Non-critical data is identified and documented
- ☐ Retention period for non-critical data meets business requirements
- ☐ Backup interval for non-critical data is within business requirements
- ☐ Data restore timeline for non-critical data is within business requirements
- ☐ Cost of potential non-critical data loss is within acceptable business limits
- ☐ Cost of non-critical data restore wait time is within acceptable business limits
- ☐ All data is stored in locations that are being backed up
- ☐ Backup test restores are planned and scheduled

NOTES:

It is important to understand that while this questionnaire and checklist will help ensure your data backup plan meets your business requirements and limits risks and costs of data loss, complete data loss prevention planning requires more than just backups.

A great onsite backup is not enough in the case of a fire destroying your office and your backup data with it.

A broken server that takes 2 days to get replaced renders your 1 hour restore plan useless while you're waiting for the new server.

If you want to minimize downtime and maximize the chances you'll recover quickly from data loss and disaster situations, you need to consider and plan for much more than just data loss prevention, such as: hardware replacement, critical services backup plans, data accessibility in case your network is down, redundancy of data and services, failover of data and services, capabilities for remote workers, policies, planning, and more…