Texas Council
Risk Management Fund

Disaster Planning – Technology Asset Inventory

This is the first part of a three-part series regarding Disaster Planning. In part one, we will discuss the Technology Asset Inventory and its role in Disaster Planning.

You have to know exactly what is affected when a disaster event occurs. One of the key ingredients of a disaster recovery plan is a technology asset inventory. The inventory should include all devices in your network, including devices such as printers, phones, and webcams. Ultimately, the technology asset inventory keeps track of what your organization is currently using to perform its daily tasks. If your system shuts down or is corrupted, knowing exactly what to replace will make the restoration efforts easier.

In a disaster scenario, an asset inventory can help pinpoint affected devices, leading to a quicker diagnosis. In cases of hardware failures, an asset inventory will allow your team to replace devices more efficiently. At a minimum, you will want to capture this basic data in your inventory:

System Type and Version
Software, including Version
Physical and Logical Location
Logical Network Addressing
Owner
Administrator
Data Sensitivity

To aid in planning, your inventory should then combine the assets captured with downtime parameters and classifications for data and hardware.

Tolerance for Downtime
Understanding your tolerance for downtime is a defining step in your disaster planning. Managers and the IT department should help to determine a recovery point objective (RPO) and recovery time objective (RTO) for your most crucial hardware and data. Your RTO and RPO define the solutions you have to adopt when dealing with downtime. Ideally, every software and hardware item would have its own RPO and RTO, so your organization can determine goals and what counts as successful recovery. When discussing downtime with upper management, remember to emphasize the fact that ordinary events happen much more frequently than natural disasters or hackers. Move the discussion away from earthquakes and hurricanes and more toward the higher probability that the location will experience a power outage or an IT hardware failure.

Classification of Data and Hardware
As you build out your asset inventory for your IT disaster recovery plan, you'll need to classify your data and applications according to their criticality. Start by speaking to your colleagues and support staff to determine the criticality of each application and data set.

Look for common areas and group them according to the criticality to your organization continuity, frequency of change, and retention policy. You do not want to apply a different technique to every individual application or dataset that you have. Grouping your data into classes with similar characteristics will allow you to implement a less complex strategy to recover.

Be wary of classifying data based on assumptions. This may haunt you eventually. Be sure to involve other business managers and support staff in this planning exercise. You will need to make some trade-offs to limit the number of data classes you have. For medium-sized organizations, the number of classes should ideally be between three and five. Different classes will have different recovery objectives. This goes back to your tolerance for downtime. For instance, a financial database may be critical to recover and have very aggressive recovery objectives because the organization simply can't afford to lose any transactions or be down for long. On the other hand, a legacy internal system may have less stringent recovery objectives and be less important to recover since the data doesn't change very often and it's less critical to get back online. This is the step where many IT departments fall short. Setting recovery objectives without consulting the organization managers is the number one cause for a plan that is misaligned from the actual needs of the organization. It's imperative that you involve them in this process to ensure the organization can recover properly during a disaster.

Here is a sample list of questions you can ask your manager colleagues:

- What applications and data does your department use?
- What is your tolerance for downtime for each?
- What is your tolerance for data loss for each?
- Are there times when these applications are not being used by employees, partners, or clients?
- Would you ever need to restore data that is older than 90 days old? How about 6 months old? How about 1 year old?
- Are there any requirements for the organization to retain the data for a designated period of time?
- Are there any requirements prevent us from moving the data from one geographical region to another?
- Are there any requirements with regard to security and encryption?

The key is to understand the needs and provide a differentiated level of service availability based on priority. This information can be translated into recovery objectives to be included in your disaster plan.

In Part-Two, we will discuss Documentation of the Plan and Achieving Buy-In from Management and Staff.

For information on the Texas Council Risk Management Fund Cyber Risk Control Program, including IT Risk Assessments, policies, procedures, and best practices visit www.tcrmf.org/cyber-security or contact Lee Cain at lee.cain@sedgwick.com.