Prompt
Read the whole prompt before you begin.

In addition to completing the preparation assignment, read over the BigU case INTRODUCTION - linked on the BigU case page.
Identify some important negative, preventable, IT-related thing that might happen to BigU.
Try to choose something you know a bit about - don't spend much time investigating, this discussion is all about speculation. :)
Required: Describe how concepts from this week's materials apply or could have been applied to your example to reduce the chance that the negative event happened or reduce the negative impact. Make sure you identify specific concepts and explain how it relates to your narrative.
Need some ideas?
Criminal gangs frequently attempt Business Email Compromise (BEC) where they send messages to employees to trick them into doing something that facilitates bad actions. For example: direct deposits for employees might be redirected.
Without proper management, BigU could squander precious funding on ineffective IT services.
Its hard to configure cloud-based services. BigU might make a mistake that exposes private information.
Ransomware gangs are prolific. Universities like BigU are constantly bombarded with efforts to compromise accounts and thereby encrypt or steal data. Extortion follows.
Individuals are subject to phishing attacks that often aim to steal usernames and passwords or even compromise dual-authentication processes. Stolen credentials can be used against BigU but may also be useful in attacking other services used by BigU people.

Primary objectives of the Plan include:
• Describe each Tier of Disruption and the preventative measures and/or mitigating controls being
taken to address the various possibilities of an unplanned outage.
• Document which key business operations are within a vendor cloud and which would not be impacted by a Tier 1 or 2 disruption within the production environment in Cloud.
• Assess preventive actions, incident management processes, and identify an organization structure
to support restoration of services for each Tier of Disruption.
• Delineate procedures that facilitate decision making to restore critical services within each TOD.
• Document and maintain changes to the specific resources needed to implement the necessary restoration of services at each TOD.
• Provide personnel information, along with supporting policies and procedures to support the recovery process.

Maintenance procedures
for the Plan are as follows:

• A major organizational change within ITwill prompt the IT VP/CIO (and/or Executive Director for TSA) to request the Director, IT to initiate a review and/or update of the BC-DR plan.
• Equipment replacement or updates which may impact the plan, along with major changes in services provided or services received, will be reviewed annually during the month of March by the Director, IT, and also require a review and/or update to the BC-DR plan.
• Any shift of an application into a vendor cloud external to the University will be recorded annually during the month of March by the Director, IT and also require a review and/or update to the BC-DR plan.
• Any determination of exposure from a cyber-attack will be reviewed annually during the month of March, and also require a review and/or update to the BC-DR plan by the Chief Information Security Officer.
• Annually, during the Summer quarter, the BC-DR plan will be organized by the Director, IT and include a table top exercise and/or DR failover test to ensure all engaged staff are appropriately informed about processes, roles, assignments, priorities, and escalations associated with the BC-DR plan.

After restoring a service failure, the BC-DR plan should be reviewed to see if information can be included in the BC-DR plan to facilitate a smoother, faster recovery, should a similar incident occur in the future.

Changes to the BC-DR plan are recorded in the Test/Maintenance Log, also included in Addendum F.