The University of Texas
Disaster Recovery Plan for Operating Technology Utilities and Energy Management

ROBERTO DEL REAL, P.E.

ASSOCIATE DIRECTOR – UTILITIES AND ENERGY MANAGEMENT

Disaster Recovery Plan

- Disasters are inevitable but mostly unpredictable, and they vary in type and magnitude.
- The best strategy is to have some kind of disaster recovery plan in place, to return to normal after the disaster has struck.
- For an enterprise, a disaster means abrupt disruption of all or part of its business operations, which may directly result in revenue loss.

Disaster Recovery Plan - Overview

This presentation discusses the approach taken for creating a sound disaster recovery plan for the UEM department at UTA.

The guidelines followed are generic in nature, therefore can be applied to any business subsystem within a university or an enterprise.

Disaster Recovery Plan - Overview

In the Operating Technology (OT) subsystem, disaster recovery is not the same as high availability.

Though both concepts are related to business continuity:

- *High Availability* is about providing undisrupted continuity of operations
- *Disaster Recovery* involves some amount of downtime, typically measured in days.

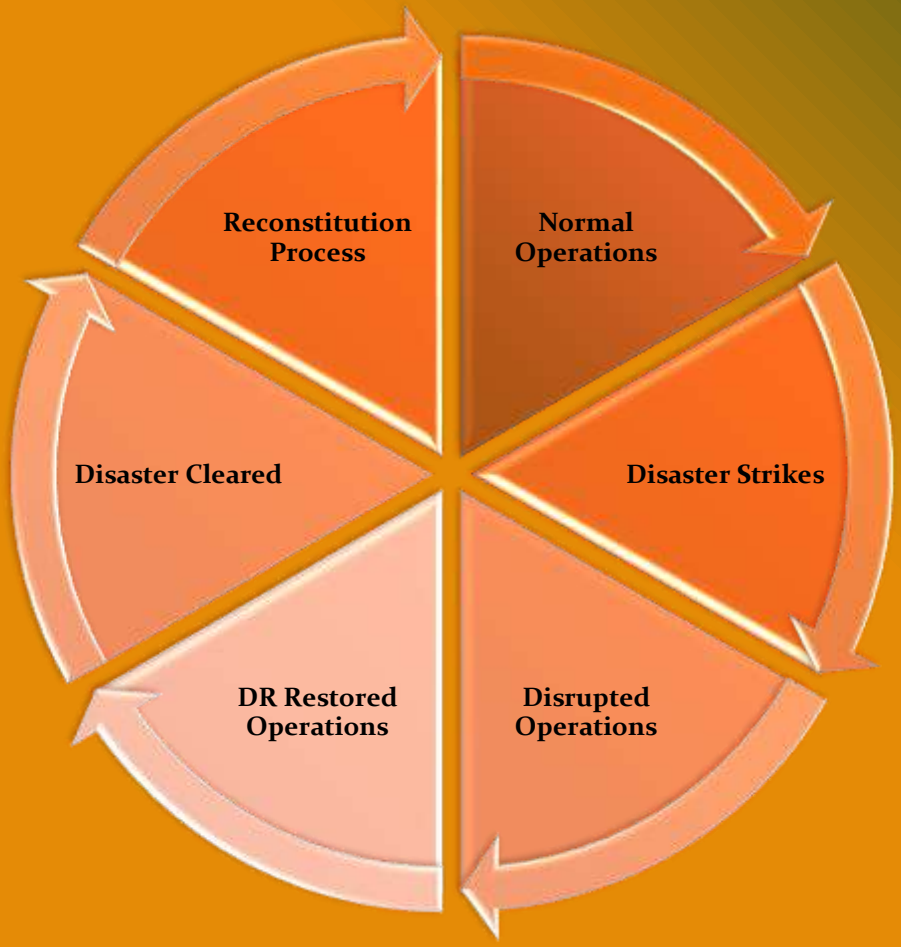
Disaster Recovery Plan - Overview

Every business disaster has one or more causes and effects.

- *Causes* can be natural or human or mechanical in origin, ranging from events such as a tiny hardware or software component's malfunctioning to universally recognized events such as earthquakes, fire, and flood.
- *Effects* of disasters range from small interruptions to total business shutdown for days or months, even fatal damage to the business.

Disaster Recovery Plan - Cycle

Cycle of stages that lead through a disaster back to a state of normalcy.



Disaster Recovery Plan - Overview

Disaster Recovery Plan should:

1) Identify and classify the threats/risks that may lead to disasters,
2) Define the resources and processes that ensure business continuity during the disaster,
3) Define the reconstitution mechanism to get the business back to normal from the disaster recovery state, after the effects of the disaster are mitigated.

Disaster Recovery Plan - Overview

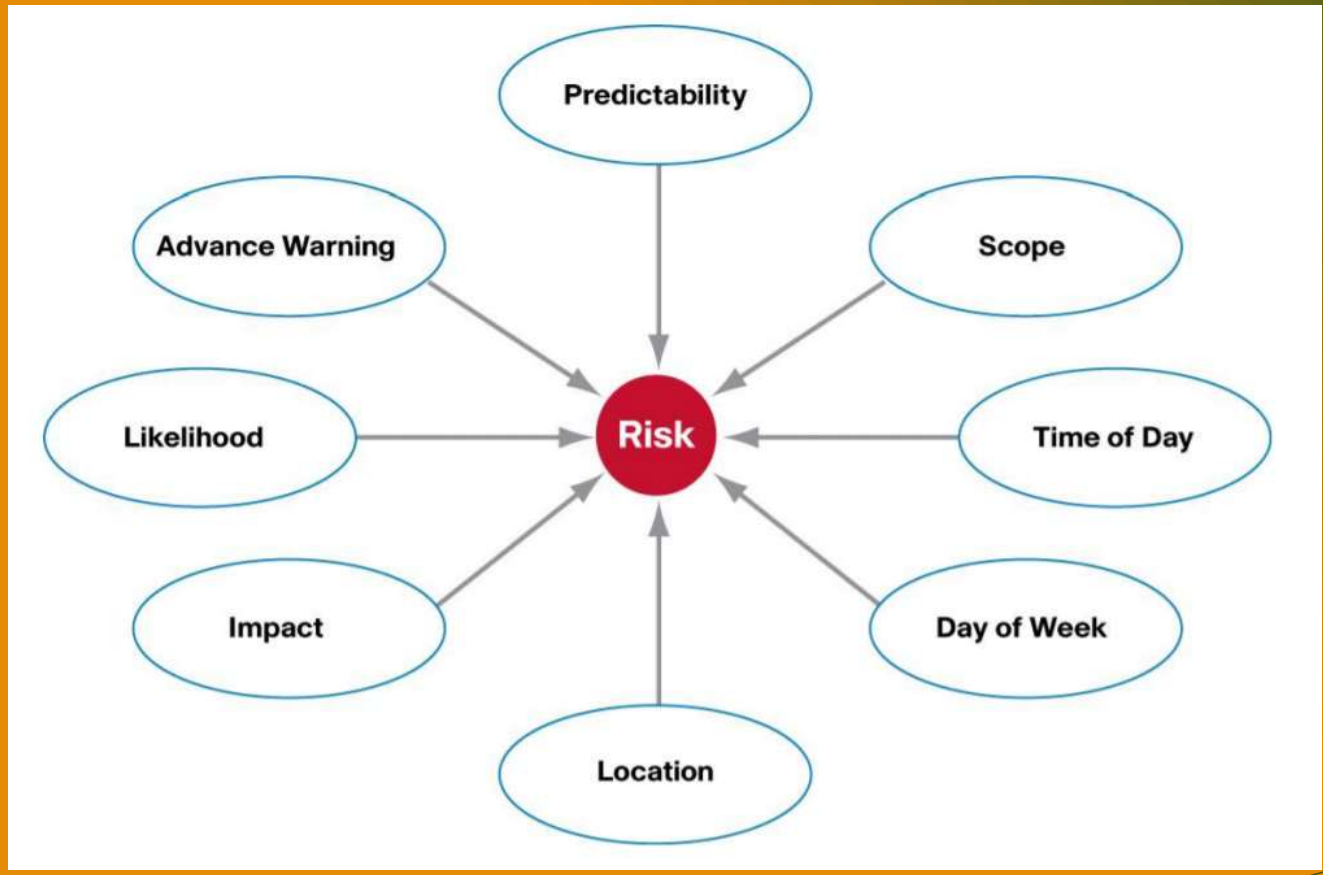
The process of preparing a disaster recovery plan begins by identifying these *causes* and *effects*, analyzing their likelihood and severity, and ranking them in terms of their business priority.

The ultimate results are a *formal assessment of risk*, a DRP that includes all available recovery mechanisms, and a formalized DR Committee that has responsibility for rehearsing, carrying out, and improving the disaster recovery plan.

Disaster Recovery Plan - Overview

The scope of a risk is determined by the possible damage, in terms of downtime or cost of lost opportunities.

For example, spilling several gallons of toxic liquid across an assembly line area during working hours is a different situation than the same spill at night or during the weekend. While the time taken and cost to clean up the area are the same in both cases, the first case may require shutting down the assembly line area, which adds downtime cost to this event.



Identification and Analysis of Disaster Risks/Threats

- External Risks
  - Natural Disasters
  - Human Caused Risks
  - Civil Issues
  - Commodities
- Facility Risks
  - Electricity Cutoff
  - Physical Security Risks
  - Climate Control
- Data Systems Risk
  - Virus
  - Software Applications
  - Data Backup and Storage
  - Data Communications/Network Loss
  - Shared Servers Risks
  - System Controllers Loss
- Departmental Risk
  - Failures within specific depts. (i.e. fire, explosion)
  - Missing door key preventing specific operation
  - Key Operating Equipment Down
  - Unavailability of Key Personnel

Identification and Analysis of Disaster Risks/Threats

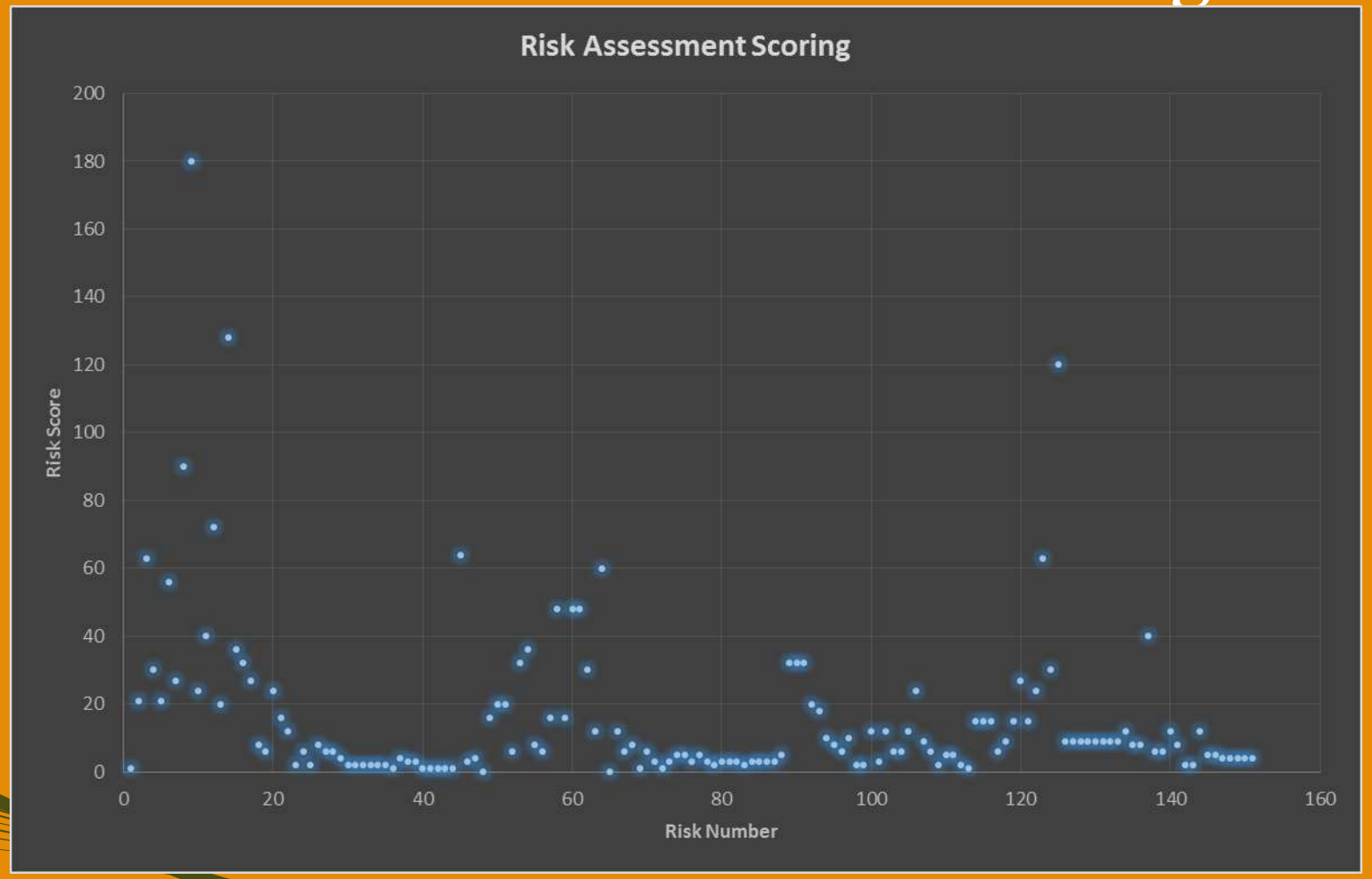
The scoring process was approached by preparing a score sheet, with the following keys:

- Groups are the subcategories of the main risk category.
- Risks are the individual risks under each group that can affect the business.
- Likelihood was estimated on a scale from 0 to 10, with 0 being not probable and 10 highly probable. The likelihood that something happens was considered in a long plan period, such as 5 years.
- Impact was estimated on a scale from 0 to 10, with 0 being no impact and 10 being an impact that threatens UEM dept. existence. Impact is highly sensitive to time of day and day of the week.
- Restoration Time is estimated on a scale from 1 to 10. A higher value would mean longer restoration time hence the priority of having a Disaster Recovery mechanism for this risk is higher.

Identification and Analysis of Disaster Risks/Threats

Risk Assessment Form						
External Risk						
Date			Likelihood 0-10	Impact 0-10	Restoration Time 1-10	Score
Grouping		Risk				
Natural Disasters Risks						
	1	Earthquake				
	2	Flooding				
	3	Tornado				
	4	Severe thunderstorm				
	5	Hail				
	6	Wildlife Intrusion				
	7	Snow/ice/blizzard				
Human Caused Risks						
	8	Sabotage or act of terror - software				
	9	Sabotage or act of terror - on machinery				
	10	Sabotage or act of terror - hardware				
	11	Campus Ingress/Egress (gameday, Campus closing due to weather)				
	12	Construction Error				
	13	Unplanned Shutdown				
	14	Water leakage in facility				
Civil Issues						
	15	Protest				
	16	Labor Issues				
Commodities						
	17	Austin Energy Power Supply				
	18	TGS Fuel Supply				
	19	Specialty Gases				
	20	Spare Critical Parts				
	21	Fuel Oil Supply				

DRP – Identification of Risks Based on Relative Weights

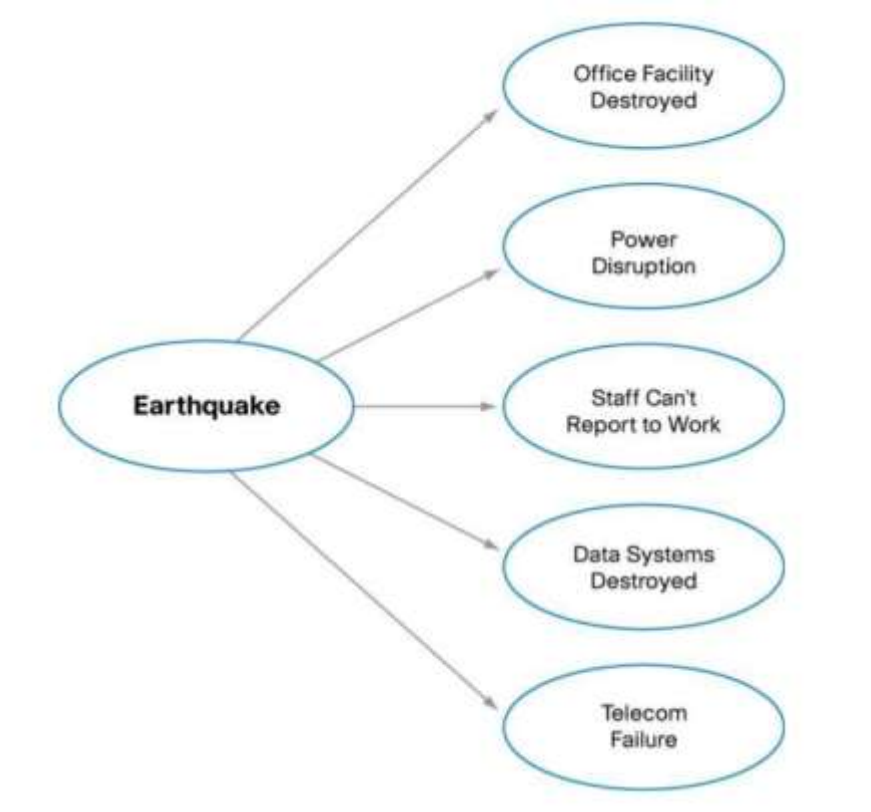


- The DRP team conducted an exhaustive risk assessment in which all risk scenarios were ranked on a 1-10 scale among three key variables: likelihood of occurrence, severity of impact, and necessary time for recovery.
- The multiplicative result of these three variables resulted in an overall risk assessment composite score and ranking.

Determining Effects of Disasters

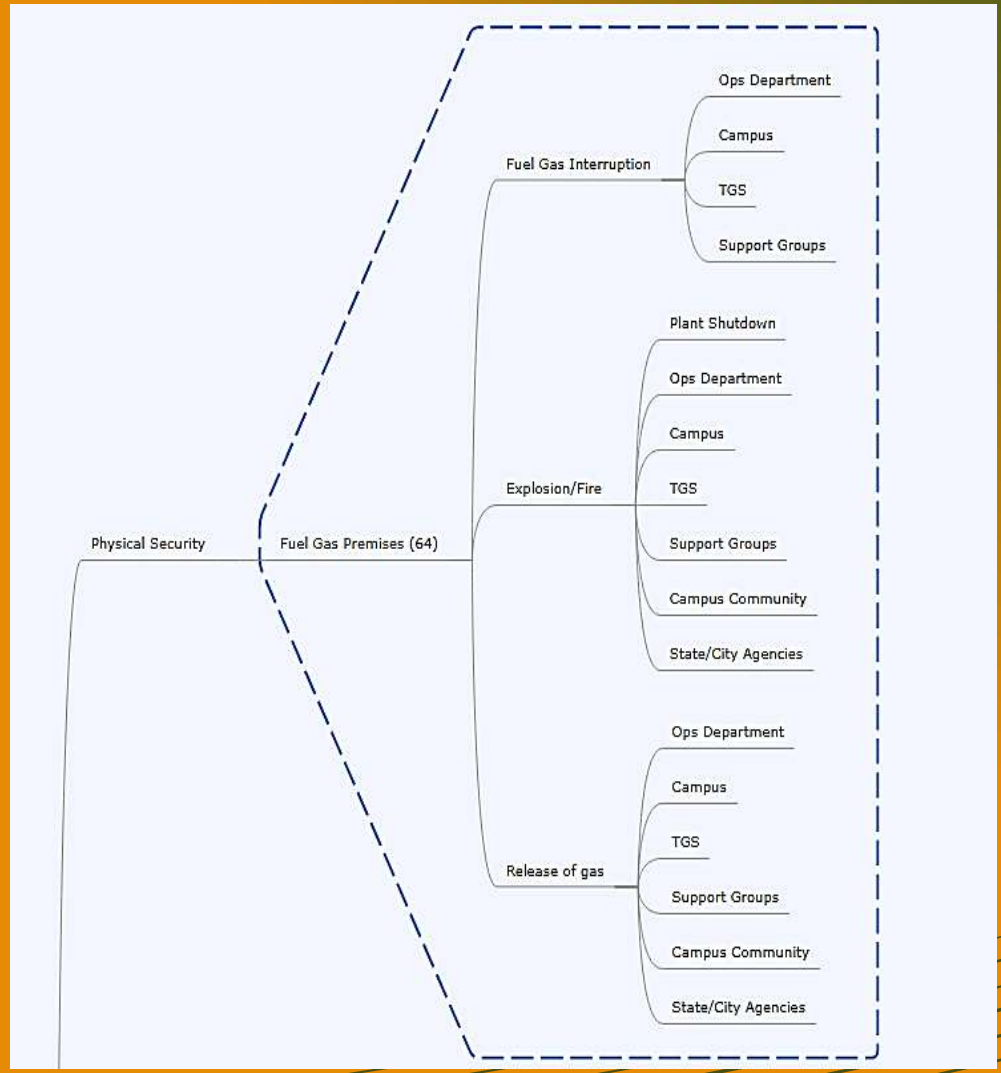
Once the disaster risks were assessed and the decision had been made to cover the most critical risks, the next step was to determine and list the likely effects of each of the disasters. These specific effects are what will need to be covered by the disaster recovery process.

Multiple causes can produce the same effects, and in some cases the effects themselves may be the causes of some other effects.



Determining Effects of Disasters

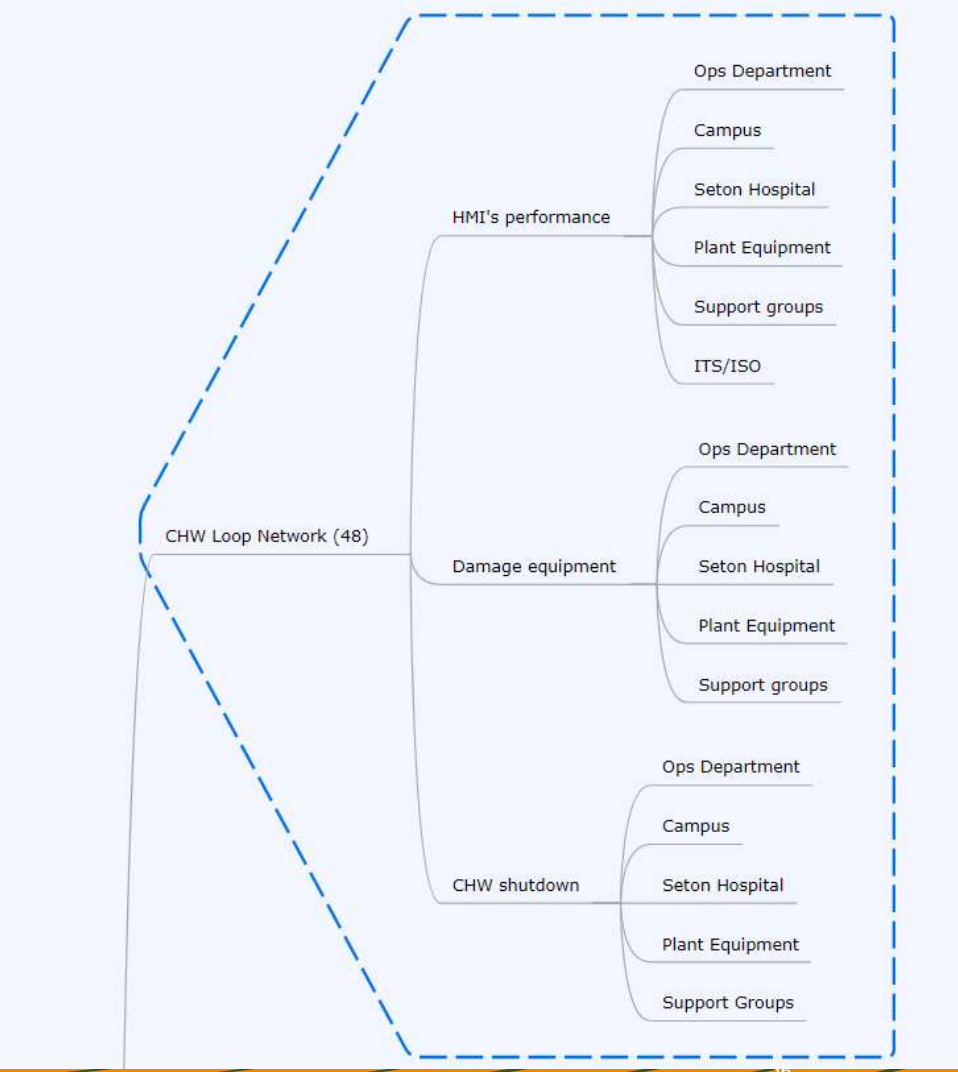
The DRP team identified over 150 specific risk scenarios during the mind-mapping phase, the team proceeded to evaluate the effects on each of the higher scored 25 risks, as well as the entities within the University that could be affected. Risks ranged from Earthquake, to software sabotage.



DRP – Evaluation of Disaster Recovery Mechanisms

Once the list of affected departments/entities was prepared and each entity's business criticality and failure tendency was assessed, the DRP Team analyzed various recovery methods available for each entity and determined the best suitable recovery method for each.

This step defined the resources employed in recovery and the process of recovery. Some of the typical entities are data systems, power, and data network systems. For each of these there are one or more recovery mechanisms in practice in the industry that UEM followed.



Disaster Recovery Committee

The Disaster Recovery Committee creates the disaster recovery plan and maintains it. During a disaster, this committee ensures that there is proper coordination between different departments and that the recovery processes are executed successfully and in proper sequence.

The Disaster Recovery Committee should be authorized and responsible for:

- Creating and maintaining the disaster recovery plan
- Detecting and announcing disaster events within the company
- Activating the disaster recovery plan
- Executing the disaster recovery plan
- Monitoring the disaster situation continuously and returning operations to normal at the earliest feasible time
- Restoring normal operations and shutting down disaster recovery operations
- Continuously improving the disaster recovery plan by conducting periodic mock trials and incorporating lessons learned into the plan after an actual disaster

Disaster Recovery Plan Document

Document Contents

The DRP-document is the only reliable source of information for the disaster recovery during an emergency. It should be very easily readable, with simple and detailed instructions.

- Document Information (i.e. authors, owners, contact details, rev. history)
- Purpose – defines objectives of plan
- Scope – circumstances under which the plan is invoked
- Assumptions – conditions the plan assumes, including dependencies
- Exclusions – related disaster activities the plan does not cover
- System Description – simple with appropriate figures
- Roles and Responsibilities – managerial and technical staff
- Contact Details
- Activation, Execution, and Reconstitution procedures
- Document Maintenance – review at least once per year

DRP -Mitigating Efforts

Roughly half of the top 25 risks are directly related to physical, network, and information/operating technology security.

As a result, related security vulnerabilities have been highly scrutinized and improved.

A lengthy development process incorporating ITS-Security, ISO, UTPD, PMCS, and several 3rd party contractors has resulted in the deployment of numerous enhancements to these critical systems.

DRP -Mitigating Efforts

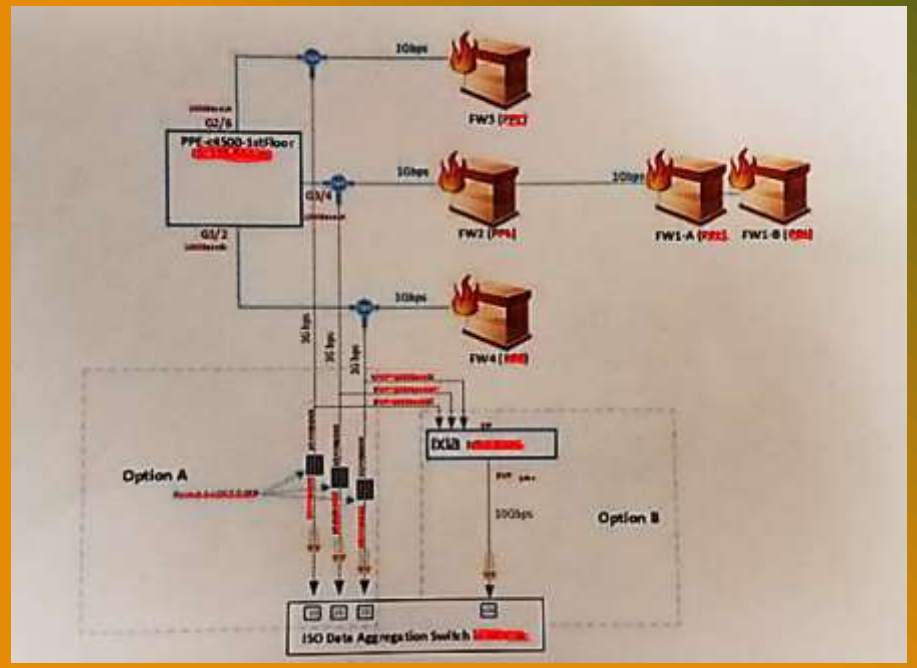
Physical security at all access points of UEM's numerous chilling station and power plant buildings were fortified by mothballing antiquated key locks in favor of modern card access in 2017, including all access points to interior control rooms and peripheral equipment rooms.

DRP -Mitigating Efforts Cyber Security

Network Security is another area where UEM, in collaboration with ITS, has made major enhancements.

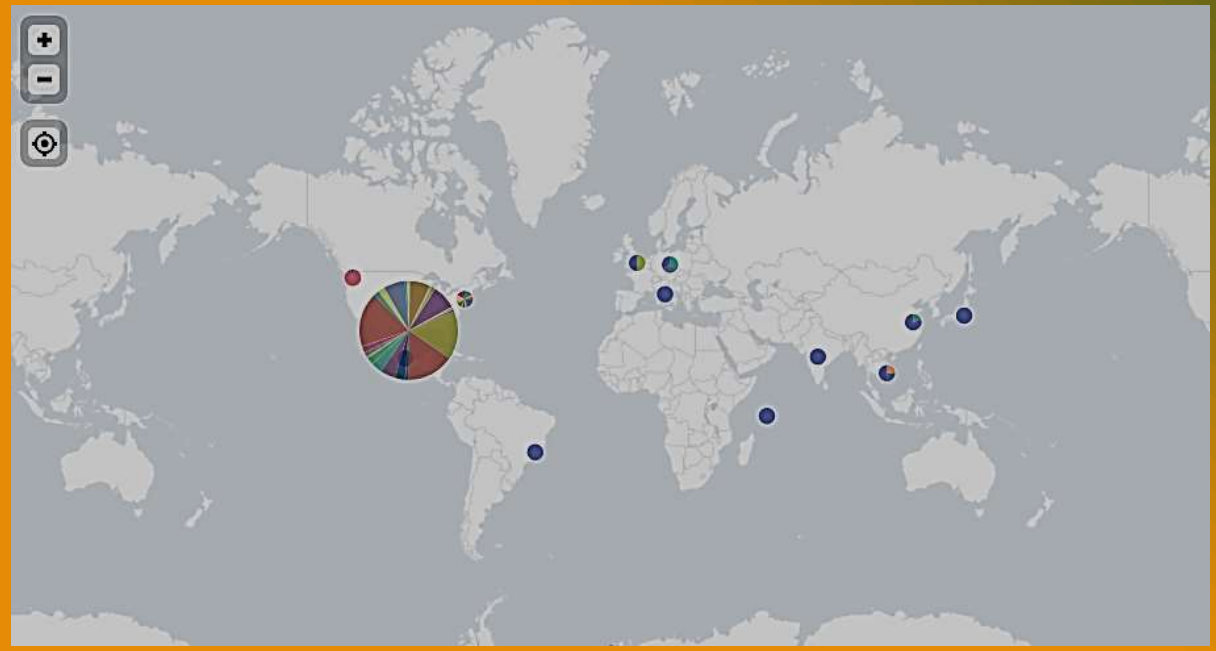
In 2016, UEM requested for ITS to analyze the UEM network infrastructure for vulnerabilities.

Network data capture and analysis has emerged as the industry best practice for effective ongoing networks security and forensics.



DRP -Mitigating Efforts Cyber Security

Information is readily available to UEM so that we can determine intrusion detection via a dashboard



Acknowledgements

Eduardo Juvera – Controls System Manager
John Fay – Controls Assistant Manager
Clay Looney – Plant Operations Manager
Mike Manoucheri – Associate Director
Nick Schroeder – Energy Manager
Akram Abderrahmani – Power Systems Manager
Eric Salazar – Electrical Supervisor
Anthony Estrada – Programmers Supervisor
Bob Hohl – Operations Supervisor - retired

Questions: roberto.delreal@Austin.utexas.edu