The Flood. 911. Anthrax. In the past year, our world has been devastated by one disaster after another. Would your organization be able to recover from disaster? What about your IS function? While all IS functions recognize the importance of planning for technical problems, how integrated is your disaster planning with the rest of the organization? Our presenters argue that disaster planning is not just the job of IS—it is the job of the organization, as a whole, to prepare and mitigate potential disasters. In the February 2002 session, the ISRC presented practical approaches to IS Disaster Planning and Recovery.

Introduction and Overview

H L Mencken, a famous journalist, once remarked, "*For every complex problem there is an answer that is clear, simple, and wrong.*" As the IS function seeks to answer the many possible problems and disruptions that can affect the way that it does business, what type of planning can be done to ensure that the answers are not clear, simple, and wrong? What steps can be taken to ensure business continuity in the face of the myriad of disruptions that threaten disaster? With three presentations from experts in the area of business continuity planning, the February 2002 session offered practical insights into how IS can prepare for the disruptive events and move this function from IS to an organization-wide effort. The 3 presenters offered their own perspective to answer this question. Each perspective will be considered, followed by an integrated approach to IS Disaster Planning and Recovery.

Perspective #1: The Portfolio Approach

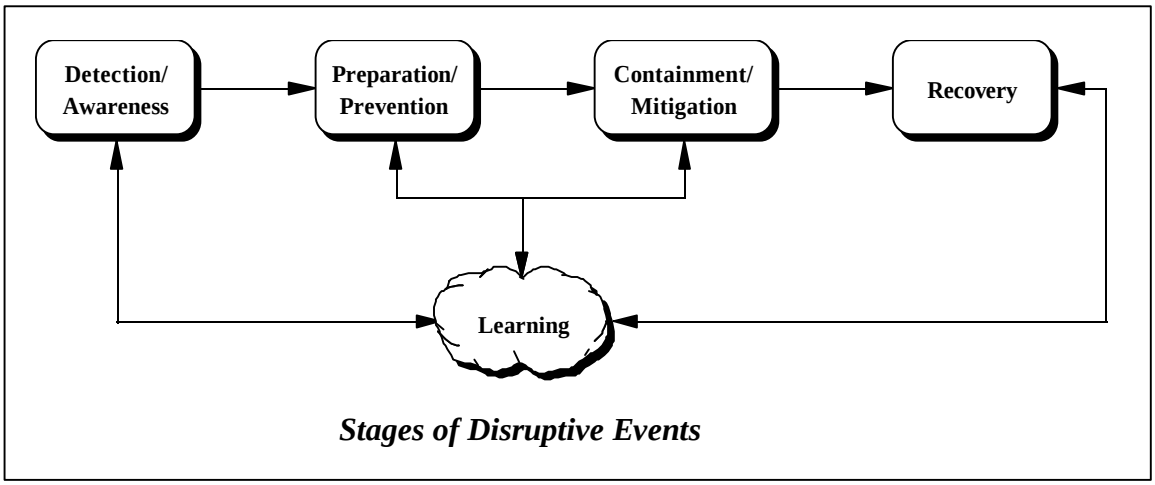
Dr. Wynne Chin, Associate Professor from the Bauer College of Business, presented an updated look at the 2000 White Paper on *Planning and Managing Information Technology in a Disruptive Environment* (if you are interested in obtaining a copy of this white paper, see the "research" link on the UH ISRC website). Using the portfolio approach, organizations should engage in 4 steps:

Step 1: Portfolio Analysis. In this step, organizations should assess the disruptive events that might impact their business. For example, in the white paper, there were over 80 possible disruptions that were identified and synthesized into 16 categories. After creating the list of disruptions, create families of events, where there are similarities. Finally, pick one representative event for each family, done by either picking the prototypical event from the category or the disruptive event most likely to occur within the family.

Then, for each family of events, create a plan for how to handle the event, using the following steps:

Step 2: Examine your preparation for each stage of the event. It is important to realize that there are multiple objectives that can be accomplished in planning for the event. Organizations must detect the disruption, prepare and prevent it, contain and mitigate as a result, and recovery. Further, learning must occur so that the organization can attempt to mitigate the effects of the

disruption in the future. The portfolio approach requires that organizations consider each family of events and create plans for each phase of the disruptive event.



Stages of Disruptive Events

Step 3: Assess capabilities. For each stage in the disruptive event, organizations should consider their capabilities in ensuring that the objective can be achieved. The capabilities can be assessed using the capabilities grid (displayed below), where the organization determines their technical, political, and cultural resources and their ability to handle each stage of the disruptive event.

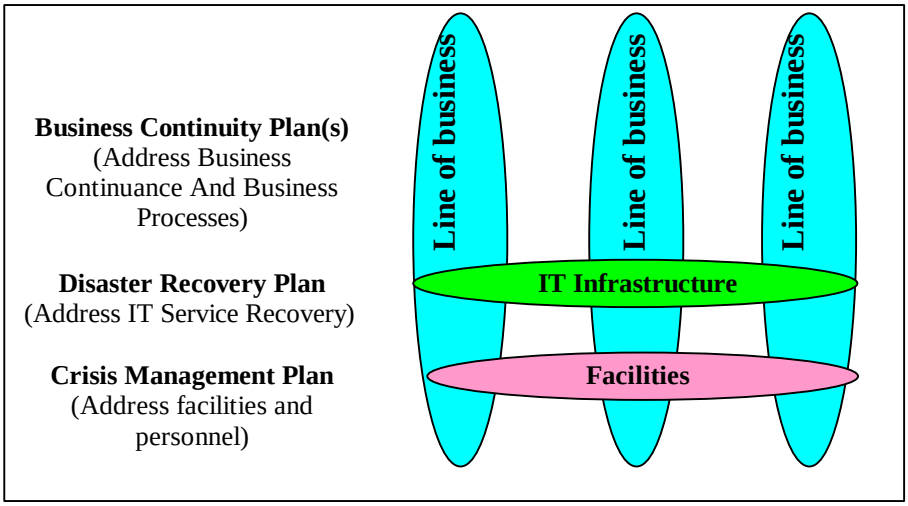
		Internal Resources		
		Technical	**Political**	**Cultural**
Event stage	Detection / Awareness			
	Preparation /Prevention			
	Containment/Mitigation			
	Recovery			
	Learning			

After examining the capabilities, the organization should create actions within each of boxes within the grid: how should the organization detect the event using technical resources? How should the organization learn from the event, given the political structure? With these actions defined, organizations can move on to the next step.

Step 4: Determine affected stakeholders. With the action steps in mind, organizations should assess how the event will affect the stakeholders, including employees, regulators, stockholders, media, competitors, management, suppliers, the union, and consumers. Determine how the action plan will affect the stakeholders and make adjustments to the plan if any of the stakeholders will adversely be affected.

Perspective #2: The Business Continuity Model Approach

Ed Haran, from KPMG, argued that disaster planning and recovery was not an IS led, but instead, an organization-led project. Organizations should establish a business continuity plan within each business unit, so that this becomes integrated within the business. The IT infrastructure should address the IT service recovery, but this is only one component of the overall approach. Facilities should also address corporate-wide issues of facilities and personnel. Overseeing this process within the organization should be a business continuity team.



The business continuity team should develop the corporate policy for business continuity and then select management within the business units to complete the tasks for the specific business units, in addition to steering corporate-wide issues of continuity, including IT infrastructure and facilities. Each business unit should then have a plan that includes:

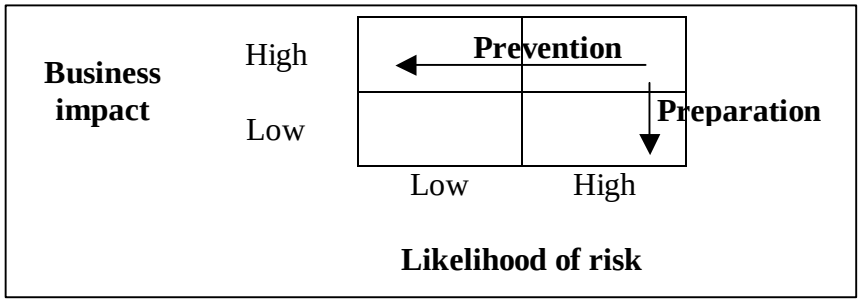
- Perform a business impact assessment for threats, defining critical processes and their contribution to the company's bottom line
- Quantify the key business processes that would be impacted by threats
- Develop a plan based upon the key business processes
- Develop communication to the employees, vendors, and public that outlines the policy and commitment to safety
- Report back to the steering committee on their processes

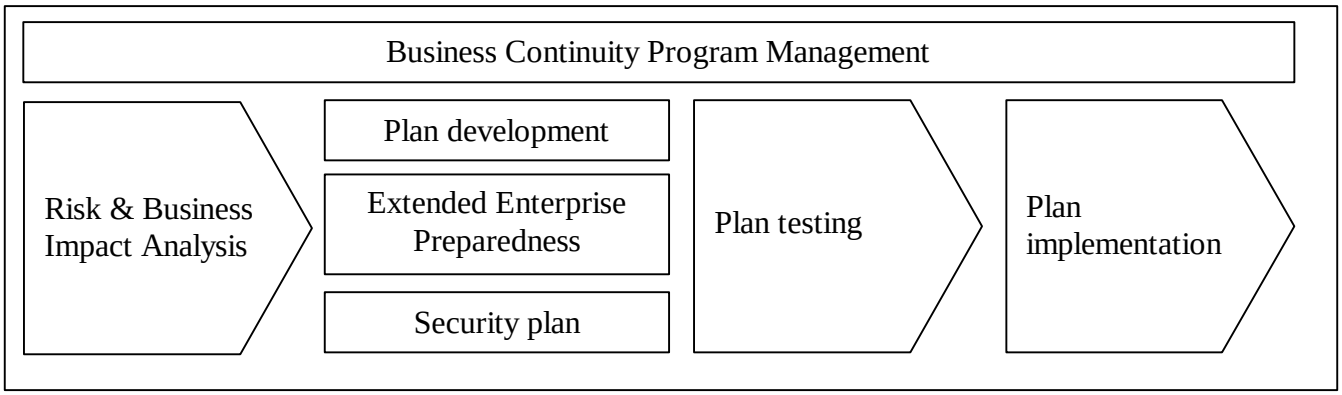
With business units owning the continuity planning, the corporation embodies a business continuity model. This evolutionary position will result in a corporation that:

- Ensures financial continuity, customer satisfaction, and productivity despite a catastrophe
- Approaches business-driven continuous availability through management of information and operational risk
- Assesses traditional threats to physical assts and emerging threats to information infrastructure
- Is enabled through emerging technologies and operational excellence

Perspective #3: The Business Impact Approach

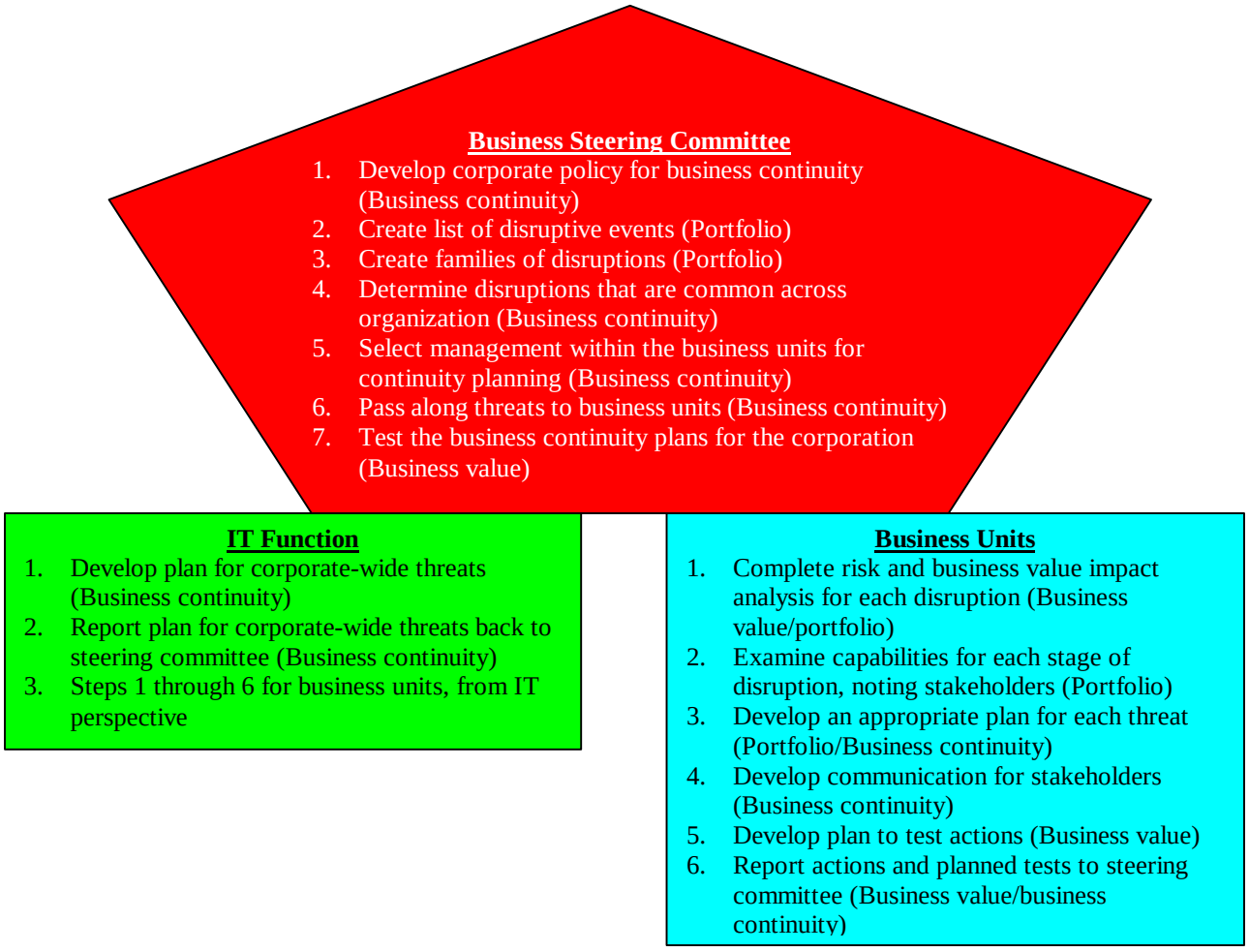
Dan Starta, from A.T. Kearney, argues that, instead of approaching disaster planning and recovery from the risk approach (e.g. the portfolio approach), the focus should be on the business impact. The disruptions that could possibly impact the business should be listed and then analyzed based upon the risk profile (depicted to the left). The goal of profiling the risks is to determine the actions that can be taken for prevention (where the likelihood of the risk occurring shifting from high to low) and for preparation (where the business impact shifts from high to low). Following the risk and business impact analysis, firms should create a plan for the enterprise, including both technical and business approaches. This plan should be tested and implemented and constantly changed, using a business continuity program management plan. The figure below depicts the business impact approach.





IS Disaster Planning and Recovery: An Integrated Approach

All of the perspectives presented during the February session are not mutually exclusive: they can be implemented in a holistic approach to business continuity. The first step is the creation of a business continuity steering committee, in charge of overseeing the corporate business continuity plan. Each business unit (including IS) must establish a structure that examines business continuity issues. These units will all be charged with responsibilities to ensure business continuity. The figure below summarizes an integrated, holistic approach to business continuity management (The words in parentheses depicts the perspective that suggests possible solutions to each step).



Conclusions

The IS function is facing many disruptions that impacts the way that it does business. However, with an appropriate business continuity planning approach that includes the suggestions put forth by the participants in the February session, the remark of H L Mencken, can be changed from "*For every complex problem there is an answer that is clear, simple, and wrong*" to "*For every complex problem there is an plan that is clear, simple, and has been tested.*" Only with proper planning can potential IS disasters be mitigated and business continuity be ensured.