Campus-wide Planning for Business Continuity and Emergency Operations

Gloria Hauck Thiele & Alan McCord
University of Michigan Office of the University CIO
EDUCAUSE 2000
Agenda

- Welcome, Overview, Icebreaker
- Campus-wide project planning: Background and context setting using Y2K
- Unique Aspects/Outcomes
- Discussion/Sharing Tools & Templates
- Examples: how to leverage gains
- Summary, evaluation, wrap-up
Purpose of the Session

- Share U-M preparedness model and lessons learned
- Learn how to leverage the Y2K success for campus preparedness
- Explore how to ensure your campus is prepared for technical outages & other emergencies
- Share successful tools, techniques, & experiences
- Take home some “how to’s”
Icebreaker Activity

• After forming small groups, introduce yourselves to each other
• Discuss, then identify the questions, issues, and desired outcomes that brought you to this workshop today
• Write each on a Post-it™ Note
• Post them on the “Questions/Issues” board

• Time - 15 minutes
Background & Context Setting: U-M Model

- Timeline /Methodology
- Project Organization
- Tools and Aids
- Emergency Operations Plan
- IT Support
“What we can’t measure are things that were built like trust, collaborations, comradery, and a better understanding from all levels, of how different areas interact, does business or just survives within the University environment.”

— Y2K school/college/unit representative
Timeline/Methodology

- Information & awareness campaign
- Unit Representative awareness and training
- Assessment completed
- Action plans developed
- Quarterly reports
- Contingency planning training
- Unit contingency plans completed
- Y2K Communication & event management plan completed
- Communication & event management plan implemented
- Emergency response team formed and trained
- Emergency response center created and activated
**Project Organization**

**Built on existing line management structure:**
- Executive Committee
- Unit Representatives
- Emergency Response Team

**Specific for this effort from UCIO:**
- Project Leader
- Communications team leadership
- Tools and Helps
Unit Representatives: Responsibilities

• Coordinate with Executive Committee to ensure unit awareness and completion of all project deliverables
• Ensure focus on mission-critical processes
• Provide information channel between units and University-wide sources
• Submit quarterly status reports
• Identify outstanding issues and action plans to resolve
Emergency Response Team: Responsibilities

- Coordinate incident response and communications
- Ensure a University-wide view of conditions
- Build on current practices making best use of exiting processes and resources
- Service Provider Teams direct response deployment within their campus operations centers
- Coordinate communications with service providers and their constituencies to coordinate a comprehensive view
Tools and Aids

- U-M Organizational Priorities defined by the U-M Executives
- Information & Awareness Campaign
- Web site
- Training sessions
- Contingency Planning
- Fully equipped EOC and secure web-based status board
Tools and Aids: Information & Awareness Campaign

- Web site
  - enhancing information and tool sharing
  - automated forms submission and reporting
  - full-phased project support and complete historical documentation
- Information and training sessions
- Extensive use of media
- School, college, unit presentations
- Community outreach
Tools and Aids: Contingency Plans

- Focused on mission-critical processes: U-M priorities
- Identified dependencies
- Developed/updated unit’s plans
- Increased communication and sharing
- Leveraged technology
Tools and Aids: Emergency Operation Center

- Documented existing capabilities & responsibilities
- Define and established a communication center to address gaps
- Fully equipped and IT supported EOC
- Automated staffing and scheduling process
Tools and Aids: IT Support

- Campus-wide Y2K web site enhancing information and awareness campaign and tool sharing
- Fully equipped EOC: telephones, radios, workstations, televisions, video
- 1-877-UM-Y2K-OK
- Conference Bridge
- Secure web-based EOC “status board”
Share Session

• Purpose: To identify additional activities from your campuses’ that can be added to the preparedness model
• Instructions
  – Identify and discuss preparedness activities
  – Write activity on Post-it™ Notes
• Share with everyone & bring Notes to facilitators
• 15 minutes
How We Benefited from Y2K

We know:

♦ how the fabric of our organization is woven together
♦ the value of information sharing
♦ how to build diverse partnerships and cooperation

We have:

♦ visibility at the top
♦ “can-do” reputation
### Unique Aspects/Outcomes

1. Finally seen not only as an IT Problem
2. Project management facilitation
3. Enhanced relationships & partnerships
4. Basis for campus Business Continuity Plan
5. Enhanced Emergency Operation Plan
6. Enhanced communication and cooperation
Unique Aspects/Outcomes

1. Seen not only as an IT Problem
   -- Loss of IT capabilities has great business process impact
   -- IT facilitated the successful response to a business/management problem
2. Project Management -- decentralized and working through exiting U-M management structures
   -- Unit Representatives
   -- Contingency Plans
   -- Communications Team
   -- Emergency Response Team
<table>
<thead>
<tr>
<th>3. Enhanced Relationships &amp; Partnerships</th>
</tr>
</thead>
<tbody>
<tr>
<td>-- Dept Public Safety</td>
</tr>
<tr>
<td>-- Risk Management</td>
</tr>
<tr>
<td>-- Plant &amp; Facilities</td>
</tr>
<tr>
<td>-- Medical Center IT</td>
</tr>
<tr>
<td>-- Faculty Leadership -- Prof. James Snyder</td>
</tr>
</tbody>
</table>
Unique Aspects/Outcomes

4. Basis for Campus Business Continuity Plan
   -- Focused on mission-critical processes:
     U-M priorities defined
   -- Identified dependencies
   -- Developed/updated unit’s plans
   -- Increased communication and sharing
   -- Leveraged technology
5. Response Center Model:
   – Response Center
     • Emergency Operations Center
     • Information Team
   – Tier 1 service providers
   – Tier 2 unit representatives
   – DPS Dispatch
   – ITCom Dial-0 operators
U-M Y2K Response Center and Tier 1 Command Centers

Tier 1 Provider

Tier 1 Provider

Tier 1 Provider

Tier 1 Provider

U-M Y2K Response Center
# Emergency Response Team Purpose

- Insure coordination and cooperation of Y2K Emergency Response Center, DPS Emergency Operations Center, and service providers’ operations centers.
- Relieve service providers of the burden to provide information to a concerned UM Community when resources will be strained.
- Insure Y2K incidents are resolved quickly.
- Insure timely and accurate communication is to internal and external stakeholders.
- Provide a well-trained and properly supplied center.
- Successful management of the rollover event.
Supporting Technologies

- U-M telephones
- Ameritech telephones
- Radio phones
- Cellular phones
- DPS dispatch
- E-mail
- Web
- Fax

- Action logs
- Status board
- Videotaping
- Cable television
  - CNN
  - Weather Channel
  - BBC
  - Local news
Unique Aspects/Outcomes

6. Enhanced Communications and Cooperation
   -- Diverse communication team of information providers from various University units
   -- Built on existing “campus watch group”
Enhanced Communications and Cooperation

- Reviewed existing processes and identified gaps
- Created integrated communication plan
- Developing matrix with key messages, audiences, vehicles and timelines
- Working with members of team University wide to disseminate key information in a timely and appropriate manner
- Provided standard press/media room environment
BREAK

15 minutes
Discussion & Sharing on Outcomes

- Identify your campus’ unique outcomes
- Discuss how these could be applied to other campuses
- Make list of additional outcomes
- 15 minutes
### OUTCOMES: What, Why, How Leveraged

<table>
<thead>
<tr>
<th>DIRECT</th>
<th>INDIRECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Business Continuity Plan</td>
<td>• Infrastructure Review</td>
</tr>
<tr>
<td>• Emergency Operations Center</td>
<td>• Security Architecture</td>
</tr>
<tr>
<td>• IT Disaster Recovery</td>
<td>• Emergency Operations Plan (EOP)</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
OUTCOMES: Business Continuity Plan

Work Group Charge:

• Ensure the maintenance of campus-wide business continuity plans to sustain critical operations in the event of a technical outage or other disaster.

• Establish an ongoing process that ensured the University is prepared through business continuity plan readiness.

• Build on and further develop information collected during Y2K contingency planning.
OUTCOMES: Business Continuity Plan

Work Group Outcomes:
• Successfully created basic procedures for business continuity planning.
• Now ready to collect information from University units and integrate into the planning materials.
• Awareness and training sessions scheduled.
### Transition from Y2K Contingency Planning: New features

- **Web site:** [www.cio.umich.edu/office/bus-cont/](http://www.cio.umich.edu/office/bus-cont/)
- **Status of business continuity planning activities**
  - Public page
  - Secure page
- **Updated supporting information**
- **Checklist and trigger information added**
- **Establishing a yearly review & updating process**
- **Year end:** Critical information linked with DPS/EOP
### Status of Business Continuity Plans in U-M Units

These plans contain confidential information. Do not share this information.
(n/a = electronic copy not available)

<table>
<thead>
<tr>
<th>UNIT</th>
<th>CONTACT PERSON</th>
<th>DATE OF CURRENT PLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Office of the President (Lee Bollinger)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>President’s Office</td>
<td>Steve Rehbo, Sherri Garff</td>
<td>December 1999</td>
</tr>
<tr>
<td>VP and Secretary of the University</td>
<td>Steve Rehbo, Nancy Asim</td>
<td>December 1999</td>
</tr>
<tr>
<td>Athletics</td>
<td>Thomas Westrick</td>
<td>December 1999</td>
</tr>
<tr>
<td>Office of the VP &amp; General Counsel</td>
<td>Catherine Rector</td>
<td>December 1999</td>
</tr>
<tr>
<td>University of Michigan - Flint</td>
<td>Vahid Drebi</td>
<td>December 1999</td>
</tr>
<tr>
<td>University of Michigan - Dearborn</td>
<td>Violette Oslyv</td>
<td>December 1999</td>
</tr>
<tr>
<td><strong>VP Communications (Lisa Rutgers)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>News &amp; Information Services</td>
<td>Julie Peterson</td>
<td>December 1999</td>
</tr>
<tr>
<td>VP Government Relations</td>
<td>Wono Lee</td>
<td>n/a</td>
</tr>
</tbody>
</table>
Business Continuity Plan Process

- Check secure Web site for unit’s current information
- Review “Update Triggers” with unit’s situation
- Review existing plan to ensure readiness (see “How to Develop a Business Continuity Plan” on web site)
- Apply Emergency Response Checklist
Business Continuity Plan Process (cont.)

- Update plan as required
- Obtain reviews and approvals
- Submit Business Continuity Plan Summary Form to “bus.continuity.reports@umich.edu”
- End of October: yearly review and update target
Tier 1 and 2 Service Providers

- Tier 1 service providers
  - DPSS
  - Housing
  - Information Technology
  - Plant
  - UMHS

- Tier 1 providers have seats at EOC

- Tier 2 service providers
  - Human Resources
  - Provost/administration
  - Purchasing
  - Regional campuses
  - Research
  - Risk Management
  - Schools/colleges/units
  - Transportation
  - Others
U-M Y2K Response Center “Tour”

- Work Area
- Information Team
- Emergency Operations Center
- Plant
- UMHS
- Housing
- DPSS
- ITD
- News & Info
- Policies
- Facilitator
- Purchasing
- Risk Management
- Transportation
- CNN
- TWC
- Status Board
- BBC
- LCL
Tier 2 Service Providers
Communication

- Tier 2 service providers per published schedule
- Constituents and/or unit representatives report to Tier 1 providers per normal procedures
- Unit representatives use hotline to Response Center for specific information
- Service providers fan-out to constituent groups per contingency plan “triggers”
- Some Tier 2 representatives may be called to Response Center per contingency plan “triggers”
Catastrophic Thinking & Practice

• “What’s the worst that can happen?” Group Discussion Exercise
• Table Top/Simulation Exercise
OUTCOMES: IT Disaster Recovery

Work Group Charge:

- Strengthen existing business continuity and disaster recovery planning efforts
- Build upon earlier work -- tool, methodology, Y2K preparedness
- Coordinate efforts with business continuity planning
OUTCOMES: IT Disaster Recovery

Work Group Outcomes:

• Central IT Service Providers stretched with Y2K and M-Pathways implementation demands
• Major IT service providers are creating project plans & timelines for the electronic capture of IT Disaster Recovery plans
• Barriers to be identified
• UMHS has and is implementing overall plan and will be cooperative partner with campus.
• Building blocks for coordinated disaster response plans
**OUTCOMES: Infrastructure Review**

*Figure 1: Michigan Model of Information Technology Services*

- **Physical Infrastructure**
  - Available
  - Cost-effective

- **Facilities and Operations**
  - Functional
  - Responsive

- **Middleware/Enabling Technologies**
  - Transferable

- **Core Applications & Services**

- **Specialized Applications & Services**
  - Sustainable
  - Cost-effective
  - Scalable

Attributes:
- Available
- Cost-effective
- Scalable
- Transferable
- Sustainable
OUTCOMES: Infrastructure Review

• Group charge
  – campus network
  – campus data centers
  – dial-up networking services
  – resident hall networking
  – high-speed connectivity to off-campus residences
  – campus computing sites
  – campus video services
  – microwave and satellite uplink/downlink services
OUTCOMES: Infrastructure Review

• How Y2K readiness facilitated the success of this effort
  – up-to-date inventories
  – current documentation
  – partnerships
  – communications
  – greater awareness of interdependencies and needs
OUTCOMES: Infrastructure Review

• Results
  – Data facility needs identified
  – Backbone upgrade proposal
  – Link to Life Sciences initiative
  – Residence Hall upgrade and bandwidth dialogue
  – Link to future construction
OUTCOMES: IT Security Architecture

Task Force Charge:

• Identify initial security architecture requirements.
• Construct a statement of principles to guide development of U-M IT security architecture.
• Develop requirements for policy changes, technical security architecture, and related actions.

Diverse membership (23)

• General counsel, risk mgmt, provost, IT providers, library, research, registrar, health services, regional campus, UCAID, UCIO
Statement of Security Principle

Responsibility for controlling access and the development and implementation of appropriate security policies, standards, guidelines, practices, and educational programs rests with the data stewards or their designees who are responsible for collecting and maintaining information as well as those charged with operating the University's information technology environments (includes all central and decentralized IT providers). The University is committed to the principle of appropriate access. For all information, data stewards should make informed decisions regarding the appropriate access that will be provided. Stewardship of the information may depend on its nature and be governed by federal laws, state laws, requirements of external regulatory organizations, and/or University policy.
### University of Michigan Information Technology Security Architecture

#### U-M Statement of Security Principle
- Limited Right to Privacy
- Technology Infrastructure
- Ownership and Stewardship of Data
- Monitoring, Auditing, and Education

#### Guidelines and Checklists for Business Owners and IT Service Providers

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptable Use Agreements</td>
<td>Risk Assessment Profile</td>
<td>Legal and 3rd Party Compliance</td>
<td>Physical Security</td>
<td>Data Classification and Stewardship</td>
<td>Backup, Recovery, Retention, Disposal</td>
<td>IT Disaster Recovery Plan</td>
</tr>
</tbody>
</table>

- Legal and Regulatory Environment
- Risks and Vulnerabilities
- Responsibility for Security
- Risk Assessment and Management

- Technology Strategy and Architecture
- University Values
- Academic and Business Processes

- University of Michigan Information Technology Security Architecture

- University Values
- Academic and Business Processes

- Risk Assessment and Management
- Monitoring, Auditing, and Education

- Technology Infrastructure
- Ownership and Stewardship of Data

- Limited Right to Privacy
- Risk Assessment and Management

- Security and Access Controls
- Technical Standards
- Business Processes
- Education and Documentation
- Self-Monitoring Processes
- Audit and Enforcement Processes

- Acceptable Use Agreements
- Risk Assessment Profile
- Legal and 3rd Party Compliance
- Physical Security
- Data Classification and Stewardship
- Backup, Recovery, Retention, Disposal

- Business Contingency Plan
- IT Disaster Recovery Plan
## University of Michigan IT Security Policy and Practice Matrix

### Security Architecture Objectives

<table>
<thead>
<tr>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish baseline global security</td>
</tr>
<tr>
<td>Minimum requirements/expectations</td>
</tr>
<tr>
<td>Determine Employee's Responsibility</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Assessment and Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability and Risk Assessment</td>
</tr>
<tr>
<td>Effective management of risk</td>
</tr>
<tr>
<td>On-going improvement of appropriate security while supporting Business needs</td>
</tr>
<tr>
<td>Support de-centralized IT providers and their business needs</td>
</tr>
<tr>
<td>Balance among Risk Management, Privacy, and Business Requirements</td>
</tr>
</tbody>
</table>

### Technology Infrastructure

<table>
<thead>
<tr>
<th>Standards-based technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portability: employee and intra-enterprise</td>
</tr>
<tr>
<td>Authentication, authorization, controlled access</td>
</tr>
<tr>
<td>Secure network and communication channels</td>
</tr>
<tr>
<td>Establish stable process environment</td>
</tr>
<tr>
<td>Physical Environments</td>
</tr>
</tbody>
</table>

### Ownership and Stewardship of Data

<table>
<thead>
<tr>
<th>Define data stewardship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsibility of data holders to data subjects</td>
</tr>
<tr>
<td>Define data classifications and responsibility</td>
</tr>
<tr>
<td>Ensure compliance with appropriate laws and regulations</td>
</tr>
<tr>
<td>Duties to 3rd Parties</td>
</tr>
<tr>
<td>Acceptable use and disposal of data assets</td>
</tr>
<tr>
<td>Retention and destruction of data/records</td>
</tr>
<tr>
<td>Acknowledge obligation to keep information timely, accurate and complete</td>
</tr>
<tr>
<td>Preserve Management's options in the event of misuse</td>
</tr>
</tbody>
</table>

### Limited Right to Privacy

<table>
<thead>
<tr>
<th>Monitoring, Auditing, Education</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education &amp; training</td>
</tr>
<tr>
<td>Monitor, measurement process</td>
</tr>
<tr>
<td>Need for periodic Risk assessment and Vulnerability assessment</td>
</tr>
<tr>
<td>Unit self-policing</td>
</tr>
</tbody>
</table>

### University Policy Standards

- Public
- Copyright not sensitive
- Strategic, Ethical, Proper
- Sensitive
- Legally restricted (FERPA, HIPAA, etc.)

### Guidelines and Business Unit Practices

- Authentication and Authorization
- Insecure Communication Channels
- Retention Guidelines
- Regents' By-law 14.07
- SPG 601.11
- SPG 601.8
- SPG 601.8-1
- Michigan FOIA

### U-M Statement of Security Principle

- Diversity of Community
- Risk Assessment
- Cost Effectiveness
- Laws and Regulations
- External Constraints
- Institutional Values
- Review Period
- Responsibility for Security
- Definitive University Community
- Limit right to privacy

### Training and Education

<table>
<thead>
<tr>
<th>Monitoring, Measurement, Tracking, Auditing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring, Auditing, Education</td>
</tr>
<tr>
<td>Unit self-policing</td>
</tr>
</tbody>
</table>
OUTCOMES: Emergency Operations Plan

- Building on partnerships developed.
- U-M Emergency Operations Plan updated to incorporate successes and lessons learned from Y2K EOC.
- Y2K EOC design became U-M EOC.
- Establishing automated information links between Business Continuity Plan and EOP/EOC.
- Plan to use IT tools and capabilities.
Share Session

• Instructions:
  – Share direct and indirect outcomes from your campus -- especially the “surprises”
  – Identify “transplant” issues to implementing models/templates on your campus
  – Discuss ways to overcome barriers

• 15 minutes
Wrap-up

- Outstanding Post-IT™ Items
- Summary
- Evaluations
- Wrap-up

Gloria Hauck Thiele: gthiele@umich.edu
AI McCord: amccord@umich.edu