Continuity State of the Union and Industry Trends

CHLOE DEMROVSKY
MADRA, FEBRUARY 18, 2016
## 2016 Trends

### Cybercrime
- cyber warfare, cyber espionage, cyber terrorism, fraud

### Supply chain disruption
- complex and long distance supply chains, just-in-time (JIT), lean manufacturing and outsourcing.

### Terrorism
- an area that is going to task emergency services, emergency planners, business continuity/resilience professionals

### Climate change
- Re: Paris agreements So how is this going to pan out? Are governments going to really support it?

### U.S. Presidential elections
- stagnation in policy change

### European stability
- financially, and results of migration from the areas that are affected by the civil war in Syria

### Asian economic stability
- issues and the fallout if the Chinese real estate and stock markets collapse

### Systemic IT failures
- business and government dependency on constant availability of IT, and possible consequences

### Regulation
- in the past, business continuity has slipped under regulator radars, but for how long?

### Risk management consolidation
- silos of business continuity and risk management, emergency management, security, etc. are going to come together.
Disaster Risk Reduction

Disaster risk reduction is the concept and practice of reducing disaster risks through systematic efforts to analyze and reduce the causal factors of disasters.

Examples:

- Reducing exposure to hazards,
- Lessening vulnerability of people and property,
- Wise management of land and the environment,
- Improving preparedness and early warning for adverse events.

(unisdr.org)
### Resilience

The adaptive capacity to maintain purpose and integrity in the face of changed circumstances.

(unisdr.org)

<table>
<thead>
<tr>
<th>Resilience</th>
<th>The adaptive capacity of an organization in a complex and changing environment. ASIS Editor’s Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a. Resilience is the ability of an organization to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event.</td>
</tr>
<tr>
<td></td>
<td>b. Resilience is the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must. (ASIS)</td>
</tr>
</tbody>
</table>

(drii.org)
Origins in Risk Management

| Risk Management | Structured development and application of management culture, policy, procedures and practices to the tasks of identifying, analyzing, evaluating, controlling and responding to risk. (UAE Standard) |

- Insurance buying
- Hazard risk management
- Scope expansion and development of the discipline since more than 30 years, but variable maturity stage by company
- Moved from protecting value to creating value through recognition of threats and opportunities in risk management
## Risk Assessment: Protecting our investments

### Location 1

<table>
<thead>
<tr>
<th>Possible Scenarios</th>
<th>Primary Workspace</th>
<th>Primary Systems &amp; Electronic Data</th>
<th>Key Personnel</th>
<th>Key Vendors and Services</th>
<th>Vital Records (Paper Files &amp; Mail)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Failure</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>G</td>
</tr>
<tr>
<td>Electric Internal</td>
<td>G</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td>Con Ed failure</td>
<td>G</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td>Back-up Generators failure</td>
<td>G</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td>Gas Leaks</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>G</td>
<td>G</td>
</tr>
</tbody>
</table>

### Telecommunications Network Failure (Lan/Wan)

<table>
<thead>
<tr>
<th>Possible Scenarios</th>
<th>Primary Workspace</th>
<th>Primary Systems &amp; Electronic Data</th>
<th>Key Personnel</th>
<th>Key Vendors and Services</th>
<th>Vital Records (Paper Files &amp; Mail)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of Vendor Service</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td>Loss of Voice Service</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td>Loss of Cellular Service</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>Y</td>
<td>G</td>
</tr>
<tr>
<td>Loss of Data Transmissions</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td>Router / Hub Failure/Firewall</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td>Overloaded: Performance failure</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>G</td>
</tr>
</tbody>
</table>

### Data Center Failure

<table>
<thead>
<tr>
<th>Possible Scenarios</th>
<th>Primary Workspace</th>
<th>Primary Systems &amp; Electronic Data</th>
<th>Key Personnel</th>
<th>Key Vendors and Services</th>
<th>Vital Records (Paper Files &amp; Mail)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software failure</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>G</td>
<td>Y</td>
</tr>
<tr>
<td>Infrastructure damaged</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>Y</td>
</tr>
<tr>
<td>Mainframe failure</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>Y</td>
</tr>
<tr>
<td>Server failure</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>Y</td>
</tr>
<tr>
<td>Router failure</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>Y</td>
</tr>
<tr>
<td>Hubs Failure</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>Y</td>
</tr>
</tbody>
</table>

### Water / Plumbing / Sprinkler Malfunction

---
Many organizations are oblivious to the threats that can destroy their business – Risk Identification and Analysis identifies and quantify these threats.

Risk management is expected for the assurance of product quality, safety and availability and ultimately, business income.

Risk management can be used as a defense against negligence.

In some countries the international or local standards are accepted as a regulatory framework.

Budget limitations require greater analytical rigor prior to the purchase of controls.

Organizations who do not follow risk management principles are likely making decisions that are too costly and ineffective.

Standard & Poors (S&P) will factor in an organization’s risk management capabilities into ratings.
How would a risk manager approach the incident?

- Facility
- Environmental
- Climatic
- Geopolitical

- Personnel
- Business
- Technology
- Operations

1. Identifies Risk/Threats
2. Frequency/Impact
3. Cost of Mitigation
4. Recommends Mitigation
Origins of business continuity

**Business Continuity**

An ongoing process to ensure that the necessary steps are taken to identify the impact of potential losses and maintain viable recovery strategies, recovery plans, and continuity of services. (NFPA 1600)

- Information technology and disaster recovery
- Physical security
Why Business Continuity Matters

• To safeguard human life
• To minimize confusion and enable effective decisions in a time of crisis
• To reduce dependency on specific personnel
• To minimize the loss of assets, revenue, and customers
• To ensure the survival of the organization
• To satisfy any legal or regulatory requirements
• To ensure that you are doing your due diligence
• To facilitate the timely recovery of critical business functions
• To maintain the public image and reputation of the organization
## Reasons for Business Continuity

<table>
<thead>
<tr>
<th>External Drivers</th>
<th>Impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demands from customers</td>
<td>Loss of customers or inability to attract new customers</td>
</tr>
<tr>
<td>Increased regulatory and self-regulated requirements</td>
<td>Regulatory sanctions</td>
</tr>
<tr>
<td>Recent Loss and/or Business Interruption</td>
<td>Audit’s recommendation</td>
</tr>
<tr>
<td>Pressure from audit committees</td>
<td>Loss of revenue</td>
</tr>
<tr>
<td>Pressure from financial institutions</td>
<td>Loss of assets and employees</td>
</tr>
<tr>
<td>Pandemic concern</td>
<td>Decrease in stock value</td>
</tr>
<tr>
<td>New threats &amp; risks since 9/11</td>
<td>Increase of insurance premiums</td>
</tr>
</tbody>
</table>

**Train. Prepare. Recover.**
Combining Disciplines

Under the umbrella of Business Continuity Management

- Business Continuity (Relocation)
- Disaster Recovery (IT Recovery and Continuity)
- Emergency Response (Life Safety)
- Crisis Management (Business Protection)

Integrated Solution
How does business continuity differ?

### 4 Categories of Problems:

<table>
<thead>
<tr>
<th>Facilities</th>
<th>Business/ Operations</th>
<th>Technology</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Fire</td>
<td>• Supply Chain</td>
<td>• Network Problem</td>
<td>• M &amp; A</td>
</tr>
<tr>
<td>• Flood</td>
<td>• Process Error</td>
<td>• Application Error</td>
<td>• Succession</td>
</tr>
<tr>
<td>• Bomb Scare</td>
<td>• Transit Strike</td>
<td>• Hardware Failure</td>
<td>• IP Issue</td>
</tr>
<tr>
<td>• SARS, H1N1, H5N1</td>
<td>• SARS, H1N1, H5N1</td>
<td>• Virus</td>
<td>• Audit Issues</td>
</tr>
<tr>
<td>• Terrorism</td>
<td>• Labor Strike</td>
<td>• Power Problem</td>
<td>• Financial Problems</td>
</tr>
<tr>
<td>• etc.</td>
<td>• etc.</td>
<td>• etc.</td>
<td>• etc.</td>
</tr>
</tbody>
</table>
How would a BC manager approach the incident?

What are the Implications of failing to mitigate or prevent?

Preparation

Structure, planning, resources, testing

Execution

Relocation, operating under duress
Two Approaches for the Same Result

<table>
<thead>
<tr>
<th>Cause vs. Effect</th>
</tr>
</thead>
</table>

**Risk Management**

- **Mitigates Causes**

**Business Continuity**

- **Addresses Effects**
Resilience through Integration

Enterprise Risk Management

Operational Risk Management

Business Continuity Management

Integrated Solution

Business Continuity

Disaster Recovery

Emergency Response

Crisis Management
Cause vs. Effect

Risk Management

- Identify Threats: Facility, Environmental, Climatic, Geopolitical, Personnel, Business, Technology, etc.
- Probability
- Cost of Mitigation
- Recommend Mitigation

Business Continuity Management

- What are the Implications of failing to mitigate or prevent
- Preparation: Structure, planning, resources, testing
- Execution: Relocation, operating under duress

RISK MANAGEMENT MITIGATES CAUSES
BUSINESS CONTINUITY DEALS WITH EFFECTS

DISASTER RISK REDUCTION MANAGES THREATS

RESILIENCE
Example: Cybercrime

- Cyber warfare, cyber espionage, cyber terrorism, fraud
- Example: Protecting the U.S. power grid
How we help

• We provide education, accreditation, and thought leadership in business continuity and related fields.
• We offer in-depth courses ranging from introductory to masters level, as well as specialty certifications.
• Founded in 1988, we are the oldest and largest organization of our kind.
How we help

- 13,000+ Certified Professionals
- Classes offered in 14 Languages
- Certified Professionals in 100+ Countries
- Courses held in 50 Countries

How we help

• We not only educate those in our field, but we also disseminate the importance of preparedness to other professions and the general public.

• We reach out and engage as many audiences as possible using broad media coverage to provide a forum for discussion.
Charitable giving and volunteerism

Vision

• Resilient communities worldwide

Mission

• To promote disaster risk reduction through partnership and education
• To aid recovery efforts through fundraising and volunteerism
Government collaboration

Europe: Disaster Management Terminology Committee with European Commission Joint Research Centre

Presented at the Interparliamentary Center for Parliamentary Studies (Belgium) and the IDRC (Davos, Switzerland)

UNISDR: Private Sector Partner

UAE: Member of Standards Committee Advisory Team

Nigeria: Participate in regular embassy drills

Malaysia: Annual DRI conference with the Ministry of Science, Technology and Innovation

Singapore: Exclusive training partner for Singapore Business Federation

APEC: Only officially recognized business continuity certification

Japan: Joint Declaration on overcoming future crises with municipal governments

United States: Chair, Alfred P. Sloan Committee to draft the Framework for Preparedness that is the foundation for the Title IX Implementation.

Member, U.S. Chamber of Commerce Homeland Security Task Force

Member, Council of Experts for ANSI-ANAB

Member, FEMA National Advisory Council Private Sector Subcommittee

Member, Advisory Committee for Congressionally funded Project for National Security Reform

Advisor, Special Assistant to The President for Homeland Security Standards Policy

DRI Canada is a member of the Technical Committee for the CSA Z1600 Standard

Mexico: National standards advisor

UNISDR: Private Sector Partner
United Nations collaboration

• We are a member of the ARISE Initiative, a Private Sector Working Group of the United Nations Office for Disaster Risk Reduction

• We represented the private sector to the UNISDR Disaster Management Terminology Committee

• Our International Glossary for Resiliency is a source document

• Research conducted in partnership with the European Commission

• We participated in the launch of the Hyogo Framework for Action 2 at the World Conference for Disaster Risk Reduction

Bottom line:
Your voice is being heard by global policymakers
Nonprofit outreach

- We are *not* a membership organization
- We partner with professional nonprofit organizations for:
  - Disseminating and sharing information
  - Networking
  - Professional education
Corporate options

Certifying individual professionals and teams:

- Nearly 80% of all 2015 Fortune 100 companies employ DRI Certified Professionals
- Over 40% of Fortune 100 companies have 5+ DRI-Certified employees
- Over half of all Fortune 500 companies have DRI-Certified employees

- **Resilient Enterprise Assessment Program**: Allows for the evaluation of BC programs within organizations and provides detailed recommendations for improvement with the goal of strengthening the programs and organizations as a whole.

- **Hub of Resilience**: Brings together community, industry, and public sector leaders to discuss how to best affect preparedness through information-sharing.
“As the certified professionals conference, you know the folks you’ll be interacting with, that you’ll be networking with, again, come with a level of experience, a level of expertise, and a level of education that are on par with a certified professional.”

March 6-9, 2016. Atlanta, Georgia.

Celebrating 5 years!

DRI 2016

The Professional’s Conference
THANK YOU

DRII.ORG

CHLOE DEMROVSKY
CDEMROVSKY@DRII.ORG
646.378.7923
@CHLOEDEMROVSKY