Corporate Contingency Planning

Theory and Practice

April 2010

Ed Halibozek
Vice President of Corporate Security
The Company - Five Operating Sectors

Aerospace Systems
- Large Scale Systems Integration
- C4ISR
- Unmanned Systems
- Airborne Ground Surveillance / C2
- Naval BMC2
- Global / Theater Strike Systems
- Electronic Combat Operations
- ISR Satellite Systems
- Missile Defense Satellite Systems
- MILSATCOM Systems
- Environmental & Space Science Satellite Systems
- Directed Energy Systems
- Strategic Space Systems

Electronic Systems
- Radar Systems
  - C4ISR
- Electronic Warfare
- Naval & Marine Systems
- Navigation & Guidance
- Military Space
- Government Systems

Information Systems
- Command & Control Systems
  - Network Communications
  - Intelligence, Surveillance & Reconnaissance Systems
  - Enterprise Systems and Security
  - IT/Network Outsourcing
  - Intelligence
- Federal, State/Local & Commercial
- Homeland Security & Health

Shipbuilding
- Naval Systems Integrator
  - Surface Combatants
  - Expeditionary Warfare Ships
  - Auxiliary Ships
- Marine Composite Technology
- Coast Guard Cutters
- Commercial Ships
- Nuclear Aircraft Carriers
- Nuclear Submarines
- Fleet Maintenance
- Aircraft Carrier Overhaul & Refueling

Technical Services
- Systems Support
  - Base and Infrastructure Support
  - Range Operations
  - Maintenance Support
- Training and Simulations
  - Technical and Operational Support
  - Live, Virtual and Constructive Domains
- Life Cycle Optimization
  - Performance Based Logistics
- Modifications, Repair and Overhaul (MRO)
- Supply Chain Management
  - Lead Support Integrator (LSI)
Corporate Contingency Planning

• Five Varied Product Operations but a Consolidated Security Focus

• Corporate Policy J1 “Security” – Seven Major Processes
  - Personnel Security
  - Information Security
  - Physical Security
  - Investigations
  - Fire Protection
  - **Contingency Planning**
  - Security Quality and Oversight

• This is the Common Charter for Security Activity in Every Sector

• Corporate Security Functions Under Enterprise Shared Services. Was Under HR Until Recently; Remains Under HR at Sectors
Corporate Contingency Planning

- Corporate Procedure – “Business Continuity Program”
  - Sub-Procedure – “Definitions” Ensures Common Terminology
  - Sub-Procedure – “Business Continuity Program Guidelines” Provides Planning Outlines and Defines Required Content

- Corporate Procedures are Supplemented and Tailored by Sectors to Address Unique Business Aspects and Issues… BUT

- A Standard Business Continuity Program (BCP) Paradigm Applies at All Company Elements

The Process
• **Crisis**: “Any unplanned event or situation, including human-caused events and natural disasters, which threatens, or has the potential, to adversely affect the business area/site as a whole in terms of its existence, reputation, values and beliefs, systems, finances, physical plant, or the medical, environmental, and emotional well being of persons within and around the facility.”

• **Crisis Management**: “A top-down, coordinated approach to provide leadership, decide policy, and direct actions to prepare for, prevent, and respond to incidents that escalate beyond the business area/site’s normal response capability.”

• **Critical Process**: “Business processes which, if significantly disrupted, would have an adverse impact on the company’s personnel, operations, revenue, customer schedules, contractual commitments, or legal obligations.”
The Wide Variety of Potential Emergencies and Business Crises

<table>
<thead>
<tr>
<th>Types</th>
<th>Natural</th>
<th>Human</th>
<th>Technical</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Medical emergency</td>
<td>Bomb threat</td>
<td>Fire (internal and external)</td>
</tr>
<tr>
<td></td>
<td>Bomb threat</td>
<td>High winds (radar range)</td>
<td>Power interruption</td>
</tr>
<tr>
<td></td>
<td>High winds (radar range)</td>
<td>Hurricane</td>
<td>Flood</td>
</tr>
<tr>
<td></td>
<td>HAZMAT spill</td>
<td>Aircraft crash</td>
<td>Snow storm/Blizzard</td>
</tr>
<tr>
<td></td>
<td>Civil disorder</td>
<td>Earthquake</td>
<td>Workplace violence</td>
</tr>
<tr>
<td></td>
<td>Terrorist threat/Attacks</td>
<td>Tornado</td>
<td>Product quality defect allegations</td>
</tr>
<tr>
<td></td>
<td>Explosion</td>
<td>Workplace violence</td>
<td>Network penetration/exfiltration</td>
</tr>
<tr>
<td></td>
<td>Law Enforcement actions (raids)</td>
<td>Tornado</td>
<td>Insider threat</td>
</tr>
<tr>
<td></td>
<td>Product sabotage</td>
<td>Product quality defect allegations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Denial of Service cyber attacks</td>
<td>Network penetration/exfiltration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intellectual property loss</td>
<td>Pandemic</td>
<td></td>
</tr>
</tbody>
</table>

Scale and Impact Define Problem & Response
Corporate Contingency Planning

- Enterprise BCP Requires Three Plans be Established, Implemented, Tested and Updated at Least Annually at Every Facility:
  - **Emergency Action Plan (EAP)** – What employees are to do in an emergency (Evacuation, Accountability, Recovery, Communication)
  - **Crisis Management Plan (CMP)** – How management structures and reacts to deal with any of the multiple types of major or more enduring crises that can occur (CM Team is Defined and Roles Established; CM Room Established; Equipment Pre-Positioned; Checklists Developed for Various Types of Crisis)
  - **Business Resumption Plan (BRP)** – How senior management returns things to normal (BR Team Defined and Roles Established; Tasks and Checklists Pre-Determined)

* Security has management responsibility
** Senior business executive has responsibility to restore business activity
Corporate Contingency Planning

• Priority is on Rapid Disaster Recovery – Physical and Cyber
  - Emergency Response: Survive and Terminate
    • React to the issue
    • Care for the people
    • Restore reasonable normalcy ASAP
  - Crisis Management: Evaluate the New Reality
    • Marshal your resources according to plan
    • Gather data and evaluate the situation
    • Organize to address changed conditions
    • Mitigate collateral fallout
  - Business Resumption:
    • Evaluate losses and quantify restoration needs
    • Tailor the plan from general to specific, test and refine it
    • Execute the plan; get back to business
Corporate Contingency Planning

• Heavy Focus on IT Security and Systems Recovery
  – All Info Systems are Subject to Business Impact Analysis (BIA) – “A documented product that assesses the value and impact of loss or delay in execution of the critical system(s) identified by functions.”

  – Critical Systems, Determined by BIA, Require an Information System Continuity Plan (ISCP) – “Sets forth the planning actions, procedures, and responsibilities necessary for the short- and long-term restoration of information systems supporting critical business operations.”

  – Test Plans are Required and Exercised for Each ISCP

  – Risk, in Lieu of ISCP, May be Accepted by Users for Less Critical Systems – But Users Must Document Their Justification for Risk Acceptance

Businesses Cannot Function Without IT
Corporate Contingency Planning

• Pandemic Preparedness – A Planning Case Study
  - Early 2006 – Corporate cadre began outlining a plan to address a potential Bird Flu (H5N1) pandemic, to address and mitigate business impacts
  - Earlier SARS concerns, and the predicted inevitability of human-to-human H5N1 infection at some point, dictated the wisdom of advance planning
  - Worldwide situation is already in Phase 3, per United Nations definition

• Pandemic Sub-Team Formed Under Hq Crisis Management Team:
  - Corporate Functions Participating: Environmental, Health & Safety, HR, Security (Chair), Travel, Law, Risk Management, Finance, Benefits, Corporate Communications, Global Supply Chain
  - Team decided advance executive planning was needed to address:
    • Medical/medication practices; Pay policy; Travel restrictions; Evacuation policies; Alternate work locations; Remote access capabilities; Alternate workforce; Quarantine & isolation policy; Allowable & mandatory time off; Return to work process; Coverage for local government lapses

Specific Proactive Planning
Pandemic Preparedness – A Planning Case Study (continued)
- Key communications: Employee awareness – potential threat; general prevention measures; preventive measures to take during Phases 4 – 6
- Identify essential employees and essential suppliers

Planning Approach – Outline Company Actions Progressively from Phase 3 (current) Through to Full Phase 6 Pandemic
- Basic Corporate Plan published in May 2006 with functional enclosures outlining specific tasks, by phase
- Plan supplements were required from all business sectors
- We continue to monitor Bird Flu status worldwide

2009 Swine Flu (H1N1) Experience Has Refined the Planning Model
- Relative virulence of a strain is recognized as a more significant factor than simple widespread prevalence, even at Phase 6
Corporate Contingency Planning

• The Ultimate Crisis – Hurricane Katrina – A Case Study

• Eight Company Locations Were Impacted in 2005

• Corporate and Cross-Functional Multi-Sector CMTs Acted
  – Assessed Needs and Coordinated Efforts to Deliver Essential Provisions:
    • Food, ice, water, fuel, vehicles, trailers, generators, forklifts, communication capabilities, payroll, physical security.
Corporate Contingency Planning

• Katrina Recovery

• Business Resilience Benefited from Having the BCP Structure in Place, from Advance Planning and applying a Flexible Focus
  – Swift and efficient action prevented worse business disruption and expedited the return to normal.
  – Within three weeks, power was restored at Ship System facilities and over 10,000 employees were back to work.
    • Remember, Katrina had impacted employee homes, families and lives.
  – Within five weeks, 12,500 employees back to work.
  – Resilience = Rapid Recovery: Benefits both customers and the company.

• Lessons Learned Were Documented – Information Shared
  – Corporate CMT began compiling experience data within 30 days of event.
  – Document shared with CMTs company-wide within 60 days after the event.
Corporate Contingency Planning

- A BCP Strategy of Partnering with Neighbors Builds Relationships
- Relationships Establish Trust and Pay Dividends
- Example:
  - NGC Corporate Hq Security partnered to develop the Century City Mutual Aid Structure
    - Focus on earthquake, fire, terrorism, civil disorder, crime
  - Worked with Los Angeles PD, Sheriff, Fire, and other Century City businesses, large and small
  - NGC hosted meetings (donuts can draw participation and make friends)
  - Helped draft and coordinate planning documentation
  - Crisis Management Teams and Control Center locations pre-planned
  - Participants and roles defined; contact lists developed
Corporate Contingency Planning

• The Future Focus – Prepare for and Prevent Major Cyber Crisis
  - Current mitigating actions
    • Consolidate corporate data centers (4) – Better control and organization
    • Decentralize locations – Spread the risk around the compass
  - Cyber Security Operations Center – A Benchmark Operation
    • 24/7/365 security monitoring of networks, servers and desktops
    • Computer security incident response and investigations provides containment, analysis and restoration
    • Digital forensics expertise
  - Cyber Threat Analysis and Intelligence Team (CTA&I)
    • **Expertise:** East Asia/China military intelligence, information warfare, advanced hacking, malicious systems and software, network security
    • **Mission:** Identify and stop the Advanced Persistent Threat (APT)
QUESTIONS?