COOP: An Overview of Cisco Federal Continuity of Operations Solutions with a Focus on Crisis Management

John Speicher
Industry Marketing Manager

FOSE
March 2006
Agenda

• U.S. Market Drivers
• Cisco’s Solution and Sales Strategy
• Network Resilience
• Application Resilience
• Communication Resilience
• Workforce Resilience
• Best Practices
U.S. Market Drivers
Primary Continuity Initiatives in Federal Government

• Civilian
  Continuity of Operations Plan (COOP)
  Enduring Constitutional Government (ECG)
  Continuity of Government Operations (CGO)

• Defense
  Defense Continuity Program (DCP)
“The purpose of...ECG...COG...and...COOP is to ensure survival of a constitutional form of government and the continuity of essential federal functions.”

Civilian Continuity Objective

“COOP planning is an effort to assure that the capability exists to continue essential agency functions across a wide range of potential emergencies. The objectives of a COOP plan include:

- Ensuring the continuous performance of an agency’s essential functions/operations during an emergency;
- Protecting essential facilities, equipment, records, and other assets;
- Reducing or mitigating disruptions to operations;
- Reducing loss of life, minimizing damage and losses; and,
- Achieving a timely and orderly recovery from an emergency and resumption of full service to customers.”

U.S. Federal Preparedness Circular FPC 65, July 26, 1999
### Key Continuity Drivers

#### Operation Forward Challenge
- Resilience/continuity capability verification
- All agencies in 2004/2005

#### Section 359—Public Law 106-346
- 25 percent/year teleworker increase mandated (+20,000 employees FY05)
- All executive agencies
- $5 million penalty to noncompliant agencies

#### COOP Directives
- U.S. Presidential Decision Directive (PDD67)
- U.S. Federal Preparedness Circular (FPC65)

#### Formal Defense Programs and Purchase Vehicles
- DCP
Cisco’s Solution and Sales Strategy
Cisco Continuity Solution
Integrated Technologies across Organization

Requirements

<table>
<thead>
<tr>
<th>Alternate Facilities</th>
<th>Interoperable Communications</th>
<th>Protect Vital Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow key staff to perform functions under various threat conditions</td>
<td>Maintain critical communications within and between agencies and to customers and public</td>
<td>Protect and enable critical information systems, applications, and records and to support agency functions</td>
</tr>
</tbody>
</table>

Continuity of Operations

- Workforce Resilience
- Communication Resilience
- Application Resilience
- Network Resilience

Integrated Security
Cisco Continuity Solution
Integrated Technologies across Organization

**Continuity of Operations**

- Workforce Resilience
  - Wired and wireless integration (campus and branch)
  - Teleworker solutions
  - Mobile worker capabilities

- Communication Resilience
  - IP Communications
  - Integrated messaging
  - Intermediate Session Routing services
  - Crisis management

- Application Resilience
  - Business-ready data-center solutions
  - Application caching (data center and branch)
  - Around-the-clock services

- Network Resilience
  - High-availability networking
  - Hardware and software availability
  - Support and services

**Technology Enablers**

- Support and services
Physical concentration increases risk
Integrated security throughout protects vital information and increases resilience
Only an integrated, government-wide architecture provides a stable foundation for enabling COOP
Network Resilience
Network Resilience Key Concern: Five-Nines Availability

Scenario

- Loss of Headquarters or Campus
- Loss of Data Center
- Security Alert (Worm /Denial of Service [DoS])

Solution

- High-Availability Networking
- Optimized Network Design
- Organization-Wide Integrated Security

Technologies

- Reliable, fault-tolerant hardware
- Optimized software and high-speed, integrated load balancing
- Advanced integrated security
- Better network operations; optimized design; fault and anomaly detection mitigation; training; best practices

Cost

Benefit

Network Resilience Key Concern: Five-Nines Availability
Comprehensive Security
Cisco’s Self-Defending Network

Cisco Strategy Improves Network’s Capability to Identify, Prevent, and Adapt to Threats

INTEGRATED SECURITY
• Secure connectivity
• Threat defense
• Trust and identity

SECURITY TECHNOLOGY INNOVATION
• Endpoint security
• Application firewall
• Secure Sockets Layer VPN
• Network anomaly detection

SYSTEM-LEVEL SOLUTIONS
• Endpoints, networks, and policies
• Services
• Partnerships
Application Resilience
Application Resilience Key Concerns

Scenario

Loss of Data Center

Loss of Application Server

Point Failure

Solution

Data-Center Mirroring

Application Balancing; Application Failover

High-Availability Hardware; High-Availability Design

Technologies

COST

- Storage area network (SAN)
- Dense wavelength division multiplexing/Coarse wavelength division multiplexing

BENEFIT

- Small Computer Interface over IP (iSCSI)/Fibre Channel over IP
- Application load balances
- Stateful failover
- Nonstop forwarding
- Smartports
Data-Center Continuity Solution Components

Government Need

- Maintain Vital Information
- Protect Information Assets Locally and Remotely
- Rapid Recovery of Mission-Critical Information and Systems
- Continuous End-User Access to Applications

Solution

- Highly Available End-to-End Data-Center Infrastructure
- Tape Backup and Remote Asynchronous Data Replication
- Synchronous Disk Mirroring and Data-Center Mirroring
- Secure VPN with IP Security (IPSec) Hardware and Load Balancing
Communication Resilience
Communication Resilience Key Concerns

Scenario

- Loss of Central Office
- Loss of Call Center
- Loss of PBX/Key System

Solution

- Distributed Central Office–Based Voice Gateways
- Distributed Call Centers
- Distributed Call Processing Survivable Remote Telephony

Technologies

- IP communications (call-processing resilience)
- IP call centers (call-center redundancy)
- Quality of Service (QoS)
- Remote management

Scenario Solution Technologies

Technologies

- IP communications (call-processing resilience)
- IP call centers (call-center redundancy)
- Quality of Service (QoS)
- Remote management
Communications Resilience—Using IP to Maintain Coordination with Multiple Failures

First Call-Center Outage
- Emergency Response 1
  - New York

Second Call-Center Outage
- Emergency Response 2
  - Washington, DC

Technology Enablers:
- Integrated Services Router
- CallManager Express
- Survivable Remote Site Telephony
- AutoQoS

Technology Enablers:
- High-Performance Routers
- CallManagers
- IP Communications Applications
- AutoQoS

Technology Enablers:
- 800 Series Router with Encryption
- IP Phones
- Remote Agent
- IP Communication Applications

Technology Enablers:
- High-Performance Routers
- CallManagers
- IP Communications Applications
- AutoQoS

Technology Enablers:
- Wired/Wireless
- SoftPhone
- Cisco Unity Personal Assistant

Technology Enablers:
- 800 Series Router with Encryption
- IP Phones
- Remote Agent
- IP Communication Applications

Technology Enablers:
- Wired/Wireless
- SoftPhone
- Cisco Unity Personal Assistant
Featured Solution—Crisis Management: Interoperable Communications

- Cisco’s continuity solution includes applications that help governments quickly respond to disruptions and threats
- Cisco MeetingPlace Crisis Management immediately connects response teams to a voice and data collaboration conferences
  
  Cisco MeetingPlace Crisis Management

  Partner services
Workforce Resilience
Workforce Resilience Solutions

• Distribution of workers among multiple sites
• Cisco workforce resilience solutions enable
  Telecommuting
  Desk sharing (hot-desking)
  Dedicated alternate sites
  Employee mobility
Workforce Resilience Key Concerns

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Solution</th>
<th>Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flood/Fire/Terrorism Loss of Physical Structure</td>
<td>Workforce Relocation To Another Facility</td>
<td>• Secure wireless LAN</td>
</tr>
<tr>
<td>Inclement Weather Workforce Cannot Go to Office</td>
<td>Dispersed Workforce</td>
<td>• IPSec VPN</td>
</tr>
<tr>
<td>Sick Child/Car Will Not Start Individual Cannot Go to Office</td>
<td>Workforce Telecommuting</td>
<td>• IP communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• QoS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Remote management</td>
</tr>
</tbody>
</table>
Workforce Relocation to Another Office: Seamless Communications

- During crises, workers can relocate to another agency facility, without IT’s help
- WLAN allows immediate application access
- Wireless IP telephony delivers immediate voice communication
- Profile migrates instantly with user
Workforce Displacement: “Office in a Box” Maintains Business Uptime

- If there are no available agency locations, set up low-cost, easy-to-deploy alternate sites anywhere with broadband Internet access

Hotel/Conference Center/Leased Space + “Office in a Box” = Instant Virtual Office
Featured Solution—Virtual COOP: Alternate Facilities

- Single connection for IP Communications support
- Centralized IT management

Agency-driven security policies (not user-managed)
Agency phone, toll bypass, centralized voice mail
Integrated security and identity services
Best Practices
Network Availability Improvement Support (NAIS): The Road to High Availability

• “Cisco’s advanced-services NAIS team provides you a roadmap to high availability, helping you achieve cost savings through operational excellence along the way.”

• Cisco offers high-availability services globally

• Cisco leading practices are proven methodologies
  Proactive network availability and network-performance management through leading practices
  Results in measurable cost savings and increased operational efficiency and availability
• High-availability network architecture meets performance and reliability goals
• End-to-end approach meets different recovery and information protection requirements
• Storage networking and metro optical technologies provide highest levels of business continuance
• Front-end and back-end strategies ensure continuous access to applications and data
• Validated solutions with storage system and management vendors facilitate deployment and support