Business Continuity and Disaster Recovery

Session 1:B
Introductions

Constantine (Dean) Macris
• Lead incident response team at Blue Team Alpha
• Instructor of Cyber Systems United States Coast Guard Academy
• United States Navy Reservist

Kristi Roose
• Iowa PCA Technology Director
• Community Hospital CIO / IT Director - Privacy Officer and Security Officer and Disaster Response Team Liaison
• Certified Professional in Health Information and Technology and Microsoft Certified Systems Administrator
Information Technology
Disaster Recovery Planning
Session Objectives

Understand what IT DRP is and where it fits in business continuity planning.

Understand physical and virtual risks to Information Technology environments.

Review components of IT DRP programs including: Business impact analysis Contingency planning Data recovery.

Understand activities needed to test, train and exercise IT DRP programs.

Introduce risk reduction programs and tools.
What is it? Where does it fit?
What is it? Where does it fit?

Disaster Recovery Planning (DRP)

Plans, procedures and resources to maintain and/or recovery the information technology systems, network, and telecommunications services.

Network

Systems and Applications

Telecom
Understanding the risks...

• Natural Hazards:
  • Meteorological (weather)
  • Iowa: 1990 – 2019, 44 presidentially-declared disasters
    • Severe weather
      • Heavy rain & flooding
      • Tornadoes & high winds
      • Ice storms
      • Blizzards & Heavy snow
  • Other
    • Hazardous material spills
    • Transportation accidents
Understanding the risks...

- Risk Assessment Template (FEMA)
Understanding the risks...

Mahaska Health

- Sunday, April 27, 2014
  - High winds & heavy rain
  - 10+ hour power outage
  - Structural failure
Understanding the risks...

**Human-Caused Hazards:**
- Accidents
- Intentional Acts – cyberattacks, violence, etc

**Technological Hazards:**
- Equipment failure
- Utility outages
- Fires, etc.
Understanding the risks...

• Human-Caused Hazard - Recent Examples:
  • Cybersecurity
    • 200 Employee Service Company
    • Ransomware Incident
    • Operating Loss $1.5M/Day
    • Legal, forensic, remediation $400k+

• Case Study
  • No plan = making it up as you go
  • Lost time in determining “what to do first”
  • Lost data encryption key
  • Incorrect order/focus on what are critical systems
  • Liability in not preserving required logs, files, drives
IT-DRP: Recovery Strategy

- Business Impact Analysis (BIA)
- Contingency Planning
- Incident Response
- Test, Train, Exercise (TT&E)
Business Impact Analysis (BIA)

NIST 800-34: 3 Steps

- **Step 1:** Determine mission/business processes and recovery criticality.

<table>
<thead>
<tr>
<th>Mission/Business Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pay vendor invoice</td>
<td>Process of obligating funds, issuing check or electronic payment and acknowledging receipt</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mission/Business Process</th>
<th>{insert}</th>
<th>{insert}</th>
<th>{insert}</th>
<th>{insert}</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pay vendor invoice</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mission/Business Process</th>
<th>MTD</th>
<th>RTO</th>
<th>RPO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pay vendor invoice</td>
<td>72 hours</td>
<td>48 hours</td>
<td>12 hours (last backup)</td>
</tr>
</tbody>
</table>

# Business Impact Analysis (BIA)

NIST 800-34: 3 Steps
- **Step 2: Identify resource requirements**

<table>
<thead>
<tr>
<th>System Resource/Component</th>
<th>Platform/OS/Version (as applicable)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Web Server 1</em></td>
<td><em>HP ProLiant ML350</em></td>
<td><em>Web Site Host</em></td>
</tr>
</tbody>
</table>

### Business Impact Analysis (BIA)

NIST 800-34: 3 Steps

- **Step 3: Identify recovery priorities for system resources**

<table>
<thead>
<tr>
<th>Priority</th>
<th>System Resource/Component</th>
<th>Recovery Time Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Web Server 1</em></td>
<td><em>HP ProLiant ML350</em></td>
<td><em>24 hours to rebuild or replace</em></td>
</tr>
</tbody>
</table>

Contingency Planning

NIST 800-34: Workbook template for Low, Moderate and High Impact Systems

3 Phases
1. Activation and Notification
2. Recovery
3. Reconstitution


Templates:
• Establish process for incident planning
• Outline Incident Detection
• Prepare for reaction to an incident
• Identify process for recovery

CMS: Chapter 08 Incident Response Planning template
Maintaining Contingency Plan and Incident Response Plans: (TT&E) Training, Testing and Exercise

- Test: Validate plan is operable. Example: does call tree work?
- Training: Informing personnel of their roles and responsibilities within a particular IT plan and teaching them skills related to those roles and responsibilities
- Exercises: Simulation of an emergency designed to validate the viability of one or more aspects of an IT plan.
  - Types:
    - Table Top
    - Functional Exercises.
- NIST SP 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
Risk reduction resources – HHS’s HICP

- Cybersecurity: HICP (Health Industry Cybersecurity Practices) HHS
  - 5 threats

<table>
<thead>
<tr>
<th>Threat</th>
<th>Potential Impact of Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail phishing attack</td>
<td>Malware delivery or credential attacks. Both attacks further compromise the organization.</td>
</tr>
<tr>
<td>Ransomware attack</td>
<td>Assets locked and held for monetary ransom (extortion). May result in the permanent loss of patient records.</td>
</tr>
<tr>
<td>Loss or theft of equipment or data</td>
<td>Breach of sensitive information. May lead to patient identity theft.</td>
</tr>
<tr>
<td>Accidental or intentional data loss</td>
<td>Removal of data from the organization (intentionally or unintentionally). May lead to a breach of sensitive information.</td>
</tr>
<tr>
<td>Attacks against connected medical devices that may affect patient safety</td>
<td>Undermined patient safety, treatment, and well-being.</td>
</tr>
</tbody>
</table>

https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
Risk reduction resources – HHS’s HICP

- Cybersecurity: HICP (Health Industry Cybersecurity Practices) HHS
  - 10 Practices
    - 89 Sub practices

https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
Risk reduction resources: NIST Cybersecurity Framework

- Outlines how to identify organizational objectives, risk appetite and resources needed

- [https://www.nist.gov/cyberframe work](https://www.nist.gov/cyberframe work)
Risk reduction resources: OCR SCR 3.0

• ONC and OCR developed Security Risk Assessment (SRA 3.0)
  • New 3.0 version – focus on small organizations
    • Includes NIST Cybersecurity Framework
    • Includes HITECH security rule & HIPAA security rule
  • New: asset tracking, vendor tracking, additional facility specific tracking
  • Coming soon: in-tool reference to NIST cybersecurity framework
  • Coming soon: scaling features to support multi-users

*** Note: Not intended to be compliance scoring tool – only risk assessment

• HRSA grant sub team discussing model for next 3 years
  • Siouxland Community Health Center
  • Crescent Community Health Center
  • CAPWN

• NIST (National Institute Standards & Technology) Computer Security Resource Center
  • https://csrc.nist.gov/publications/sp
  • NIST CyberSecurity Framework: https://www.nist.gov/cyberframework
  • Crosswalk NIST security framework to HIPAA security rule

• Department of Homeland Security – Ready.gov
  • https://www.ready.gov/business/implementation/IT

• HICP (Health Industry Cybersecurity Practices)
  • https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
    • Framework available for small healthcare organizations
    • https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
      • Crosswalk to HIPAA security rules
      • If outsourcing IT services - specific guide released this month HIC-SCRiM
        • https://healthsectorcouncil.org/HIC-SCRiM/

• OCR SRA tools:
Contact Us

Kristi Roose
Technology Director
Phone: 515-333-5040
Email: kroose@iowapca.org

Dean Macris
Title
Phone:
Email:

facebook.com/iowapca
twitter.com/iowapca
youtube.com/iowapca
www.iowapca.org