Building an Effective Cyber Exercise

Richard Long, Senior Advisory Consultant, MHA Consulting

January 10, 2018
18-year proven track record of applying industry standards and best practices across a diverse pedigree of clients.

A simple mission: Ensure the continuous operations of our clients’ critical processes.

60% of revenue comes from Business Resiliency, 30% from IT Disaster Recovery, and 10% from SaaS tools.

SaaS Tools: BIA On-Demand, Compliance Confidence, Residual Risk.

MHA Consulting’s senior team has an average of over 20 years of industry relevant experience in the areas of Business Continuity, Disaster Recovery, and Project Management.

Richard Long, Practice Leader & Senior Advisory Consultant Phoenix, Arizona
www.mha-it.com
DIVERSE, GLOBAL CLIENT BASE

<table>
<thead>
<tr>
<th>SERVICES</th>
<th>HEALTHCARE</th>
<th>EDUCATION</th>
<th>FINANCIAL INSTITUTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Early Warning</strong>, LifeLock, AMGEN, CVS Health</td>
<td><strong>Coviden</strong>, NuVasive, McKesson, Medtronic, Phoenix Children's Hospital</td>
<td>ASU, Maricopa Community Colleges, Johnson &amp; Wales University, The Catholic University of America</td>
<td>American Express, PenFed Credit Union, City National Bank, Charles Schwab, Desert Schools Federal Credit Union, Fannie Mae, Square, Mercedes-Benz Financial Services</td>
</tr>
<tr>
<td>TRANSFRACT, Hewlett Packard Enterprise, kw Keller Williams, Zacks</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CONSUMER PRODUCTS</th>
<th>INSURANCE</th>
<th>TRAVEL &amp; ENTERTAINMENT</th>
<th>GOVERNMENT/UTILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>BJ's, Rattner Companies, GameStop, Insight, Guitar Center</td>
<td>Mutual of Omaha, Health Alliance, CopperPoint, York, SkyWest</td>
<td>MGM Resorts International, Harrah's Entertainment Group, Regal Entertainment Group, AAA, AAA, City of Tempe, Arizona, PNM, CAP, NASA</td>
<td></td>
</tr>
</tbody>
</table>
## Robust Suite of Services

### Assess the Current Environment
- Current State Assessment
- Policy & Standards
- Business Impact Analysis
- Threat & Risk Assessment
- BCMMETRICS™ BIA On-Demand (BIA<sup>OD</sup>)
- BCMMETRICS™ Compliance Confidence (C<sup>2</sup>)
- BCMMETRICS™ Residual Risk (R<sup>2</sup>)

### Recovery Strategies & Solutions
- Business Recovery Strategies & Solutions
- Data Center Recovery Strategies

### Response & Recovery Plans
- Crisis Management
- Business Recovery
- IT Disaster Recovery

### Exercises
- Training & Awareness
- Mock Disaster Exercises
- Plan Functional Walkthroughs
- Alternate Worksite Exercises

### Maintain & Improve
- Update Recovery Plans
- Update Current State Assessment
- Update Business Impact Analysis & Threat Assessment
- Third Party Assessments
### BCM COMPLIANCE STANDARDS

<table>
<thead>
<tr>
<th>STANDARDS IN BUSINESS CONTINUITY</th>
<th>MEASURE COMPLIANCE IN THESE BCM DIMENSIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• ISO 22301</td>
<td>• Program Administration</td>
</tr>
<tr>
<td>• FFIEC</td>
<td>• Crisis Management</td>
</tr>
<tr>
<td>• NIST 800</td>
<td>• Business Recovery</td>
</tr>
<tr>
<td>• NFPA 1600</td>
<td>• IT Disaster Recovery</td>
</tr>
<tr>
<td>• SEC</td>
<td>• Fire &amp; Life Safety</td>
</tr>
<tr>
<td>• FISMA</td>
<td>• Supply Chain Risk Management</td>
</tr>
<tr>
<td>• FINRA</td>
<td>• Third Party Management</td>
</tr>
<tr>
<td>• Supply Chain Resiliency Leadership Council</td>
<td></td>
</tr>
</tbody>
</table>
Why Are You Here?

- What & Why of Cyber Exercises
  - Scope
  - Who should participate
  - Types of exercises
- How of Cyber Exercises
  - Planning
  - Managing the activities
- What to Do With the Results
**Business Resumption Planning**

- The process initiated to resume business operations to a level consistent with the business requirements.

**IT Disaster Recovery Planning**

- The recovery of information technology processes, systems, applications, databases, and network assets used to support critical business processes.

**Crisis Management**

- A series of actions taken to gain control of the event quickly to minimize the effects of an interruption and prepare for recovery.

---

**SO, WHAT IS BUSINESS CONTINUITY MANAGEMENT?**
DEFINITIONS

**Business Continuity**
Overall continuation of business functions during an emergency event.

**Disaster Recovery**
Recovery of systems, applications, and processing capabilities.

**Process**
A business process is functional and available; remains available even during potential impact events.

**Application**
Available for use by the organization based on requirements; remains available even during potential outage events.
“On one hand, I’m grateful that we’ve never been targeted for a cyber-attack. On the other hand, I’m insulted that nobody thinks we’re worth the effort!”
BASIC COMPONENTS IN CYBER PLANNING

01 CRISIS MANAGEMENT. The tasks and actions taken to manage an event. Plans should include specific sections on cyber events. Include third party assistance.

02 IT CYBER PLAN. Similar to the IT Disaster Recovery plan; a plan related to IT actions and procedures for cyber events. Include third party assistance.

03 STRATEGY/IMPLEMENTATION. Technical implementation.

04 CYBER TESTS. Verifying strategy and management are functional.
WHAT IS A CYBER EXERCISE?

FIND ISSUES OR GAPS

• Reality-based scenario requiring technical and non-technical response & actions related to any cyber or potential cyber breach (data loss, ransomware, virus, etc.).
• Opportunity to validate the technical response strategy and details.
• Training opportunity for technical staff.
• Training opportunity for business personnel.
• Training opportunity for emergency management of the event.
• Opportunity to identify gaps and weaknesses in the recovery strategy, implementation, procedures, and dependencies.
WHAT IS A CYBER EXERCISE?

NOT A SUCCESS OR FAILURE

• An EXERCISE is **not** binary.
• Success means being able to react appropriately NO MATTER HOW MANY ISSUES OCCUR.
• Success means finding areas of improvement and issues to resolve.
• Success means improved training and knowledge.
• Failure = No issue; everything was perfect.
  • Impossible (almost) to be true
• Failure = Not being able to perform any recovery or only talking “theoretical”.
TYPES OF CYBER EXERCISES

THERE IS NOT ONE TYPE

- Technical Exercises
  - Validating technical components and performance
- Business (Non-Technical) Exercise
  - Functional impacts
  - Communication (Internal & External)
- Organizational Management/Crisis Management
  - Overall management of event
- Including Third Parties
  - Law Enforcement
  - Security Consultants
- Combination of all of these
TYPES OF CYBER EXERCISES

SCENARIOS

• Data Breach
  • Private, confidential, personal data leaving the premises; may be electronic or physical
  • Ransom/vendetta of data obtained
• Malware/Ransomware
  • Data corrupted/encrypted
  • Requires paying actor to unencrypt data
• Malware/Virus
  • Server impacting
• Phishing access
  • Which leads to above
• DDOS – Denial of service
Planning is not about Cyber Implementation.

• Should not be about finding gaps and correcting them before the exercise.
• Should not be about making sure the exercise is a "success."

PLANNING FOR THE EXERCISE

PLAN – DON’T IMPLEMENT
PLANNING FOR THE EXERCISE

PREPARE – DON’T OVER PLAN

Planning = Organization

• Determine type of exercise.
• Buy-in from management.
• Identify and schedule the participants.
• Communicate scope and execution expectations.
• Ensure there is no production impact.
• Identify potential impacts which may be major roadblocks that stop the exercise.
• Action item identification and follow-up.
• Organize resources and schedule time.
  • Third Parties
• Develop exercise schedule.
  • People Schedule
THIRD PARTIES

WHO DO YOU INCLUDE?

- Law Enforcement
  - Local
  - Federal (FBI)
- Insurance
- Security consultants/partners
- Technical partners
  - Storage/Server/Network
  - Monitoring
- PR/Communication firms
WHAT IS APPROPRIATE SCOPE?

• Technical Exercises
  • Simulate the scenario and execute troubleshooting or research.
  • Identify actions.
• Business (Non-Technical) Exercise
  • Scenario based to force use of workarounds or BC plans.
• Organizational Management/Crisis Management
  • Use different scenarios, not just data breach of PII.
• Increasing complexity or impacts
WHO ARE THE PARTICIPANTS?

TECHNICAL & BUSINESS

• Crisis Management
• Infrastructure (Network/Storage/Server)
• Security (both IT and Physical)
• Risk Management
• Local
COMMUNICATION & DISCIPLINE

- Ensure disciplined actions:
  - Use documentation, not memory
  - Communicate at each major milestone
  - Communicate all issues no matter how small
- Use of timeline
- Single source of status & updates
- Keep it real
- Execute in real time if possible
MANAGING THE EXERCISE

Consider:

01 Pre-Start Meeting – Remind about communication methodology and execution expectations.

02 Online tool/sharing.
   • Consolidated Issues List
   • Schedule and Recovery Status

03 Regular Status Meeting.
   • Leaders provide status, not those performing the recovery
   • Prevents distractions to technical staff

04 Remind and follow up on use of documentation and identification of issues.
   • Focus on identification of issues, not binary results.

05 Single Coordinator.

06 Follow-up on issues/action items identified.
HOW CAN YOU PERFORM MORE THAN ONE?

- Perform a single large integrations-based exercise annually.
- Perform component exercises monthly/quarterly.
  - Technical
  - Crisis Management
  - Business
- Short (5 – 15 min.) exercises in staff meeting.
WHAT TO DO WITH THE RESULTS

01 ADJUST THE STRATEGY. May require modifications to the recovery strategy based on results and needs.

02 ADJUST RECOVERY PROCEDURES & DOCUMENTATION. A major benefit is updating and ensuring functional procedures and actions.

03 REVIEW & UPDATE COORDINATION WITH BC PLAN. Review and validate the integration and validity of BC plans while recovery occurs.

04 BUDGET. Honest results help in determining both budget and approval from management.

05 ACTION ITEMS. Identify and manage actions from the exercise to improve and ensure functional capability.
SO, WHAT ARE THE NEXT STEPS?

WHAT DO WE DO NOW?
HOW DO WE START OR CONTINUE?

Identify when the last actual exercise occurred. Do you know the results of the last exercise?

Perform a crisis management exercise.

AREAS TO REVIEW
WHERE TO PRIORITIZE

• Crisis Management Plan
• Communication Plan
• Technology Solutions

• People know what to do
• Training of all staff on risks
• Validate current state
FINAL THOUGHTS

IT’S NOT IF, BUT WHEN