What the Disaster Taught Us – Webinar #3

Tom Williams – Business Continuity Strategy Manager
Debbie Dissinger – Chief Operations Officer - Peoples Security Bank & trust
Susan Hubble – Vice President, IT – Peoples Security Bank & Trust

Presented by
Jack Henry & Associates (Gladiator Division)
Next in our Maturing Your Cybersecurity Program series:

**Webinar 4:**

*What Can You Expect Next – Cyber Threats and Trends in 2019*

Wednesday, January 30, 2019 at 2 p.m. ET
Previous Webinars in our: Maturing Your Cybersecurity Program Series:

Webinar # 1
How our Bank Successfully Implemented a Virtual Information Security Officer
Presented by: Viviana Campanaro and Tom Williams, Gladiator
Featuring Sue Ozburn, Cashmere Valley Bank

Webinar #2
Evaluating Your Cybersecurity Program
Presented by: Viviana Campanaro – CISSP
Webinar Objectives

- Express the importance of preparation and having an effective Business Continuity Plan (BCP)
- Provide information to *measure* and *strengthen* your Business Continuity Plan
- Provide *lessons learned* from a bank based on their recovery experience of an actual disaster event
In the News
Can your Financial Institution pick-up the pieces after a major disaster?
Every business is at risk from potential disasters...

- Natural Disasters, Accidents, & Environmental Events
- Terrorism & Cyber Attacks
- Power & Energy Disruptions
- Telecommunications & Equipment Failures
- Infectious Diseases
- Human Error
What is your Financial Institution’s Disaster Risk Mitigation Profile?

Effective BCP

Low Risk

SEMI-LOW

MODERATE RISK

SEMI-HIGH

No BCP

High Risk

Each organization should continually strive to move toward the Low Risk area
Business Continuity Planning Challenges

- Lack of management support/budget restraints
- No formal process for BCP program
- Meeting FFIEC regulatory guidelines
- Ongoing plan testing/maintenance at all levels
- Lack of training and business continuity awareness
- Not knowing when to ask for help from experts
The Business Continuity Plan Life Cycle and Components
Plan Maintenance
- Phased approach
- Tabletop exercises
- Mock drills
- Functional testing

Documentation
- Emergency Management Plans
- Crisis Management Plans
- Business Unit Plans
- Incident Response Plan

Risk Management

Risk Monitoring

Risk Assessment

Business Functions
- Recovery Window
- Resources
- Contingency Strategies
- Impact

Threats
- Natural
- Human
- Technical
- Cyber

BCP Lifecycle
People

Facilities

Technology

+ A Plan That Ties It All Together
V. IF YOU EVACUATE

Take with you:

- Medicines and first aid kit
- Flashlight, radio and batteries
- Important documents and cash
- Blankets and extra clothes
- Personal sanitary items
- Any additional items you feel are necessary
Documentation

Emergency Management Plans
• Evacuation procedures
• Scenarios

Crisis Management Team Plan

Business Unit Recovery Team Plans
Team Responsibilities

- **CRISIS MANAGEMENT**
- **MANAGEMENT**
- **ADMINISTRATIVE**
- **DAMAGE ASSESSMENT**
- **INFORMATION SYSTEMS**
- **BUSINESS UNIT RECOVERY**
- **BUSINESS UNITS**

Business Units

- Recover business functions
  - Relocate to assigned workspaces
  - Acquire and restore resources
  - Recreate lost work
  - Implement Contingency Strategies
Executing and Testing the Plan
Recovery Phases & Plan Execution

RECOVERY TIMELINE
Recovery Phases & Plan Execution

1. CRISIS MANAGEMENT

- Evacuation & safety
- Liaison
- Stabilize
- Incident Response
- Damage assessment
- Communications
- Disaster declaration
Recovery Phases & Plan Execution

1. CRISIS MANAGEMENT
   - Notifications
   - Salvage
   - Establish Command Centers
   - Determine alternate workspaces
   - Acquire resources
   - Restore resources

2. RELOCATE & RESTORE
Recovery Phases & Plan Execution

1. CRISIS MANAGEMENT
   - Recreate lost work
   - Implement contingency strategies
   - Resume business functions

2. RELOCATE & RESTORE

3. RECOVER BUSINESS FUNCTIONS
Recovery Phases & Plan Execution

1. CRISIS MANAGEMENT
   - Repair or replace damaged equipment and/or facilities
   - Formulate a plan for returning to normal operations
   - Execute the plan
   - Perform a debrief session

2. RELOCATE & RESTORE

3. RECOVER BUSINESS FUNCTIONS

4. REBUILD & RETURN
Business Continuity Plan Maintenance Process

- Locations, Personnel, Recovery Teams, Departments
- Business Functions, Process, Resources
- Vendors, External Contacts
- IT & Application Recovery Procedures
- Custom Documentation
- Testing
Business Continuity Plan Testing Process

- Adjust and Retest
- Compare Results with Objectives
- Conduct Test
- Test Plan
- Identify Scope
- Identify Participants
- Set Test Objectives
- Select Training Methods
- Identify Resource Requirements
Customer Profile: Peoples Security Bank & Trust – Scranton, PA
Peoples Security Bank & Trust

• Location: Scranton, PA
• Asset Size: $2,233,459,000
• Employees: 416
• Branch Locations: 27
• Business Continuity Plan: Centurion BCP Service
Peoples Security Bank & Trust – Technology Profile

- Core: Silverlake in house
- Centurion Disaster Recovery Services
- Centurion Business Continuity Plan Development Service
- Gladiator vISO (Virtual Information Security Officer)
- Gladiator ISABRA (Information Security Asset Based Risk Assessment)
- Gladiator MITS (Managed IT Services)
- Jack Henry Call Center with our Cisco phone system
- Two data centers 50 miles apart with branches connecting to each. jConnects and FED VPNs in each
Our Business Continuity Plan
Our Business Continuity Plan (BCP)

• Built and maintained using the Centurion’s Web Hosted BCP Software Tool (COPE). Set up COPE in June 2017.
• Migrated from Word BCP document to a living, breathing application in COPE.
• Business owners were identified and given COPE logins.
• Any time a process changes they update their own processes in COPE.
• The new question during meetings is “did you COPE that?”
• All business processes are documented, not just the critical ones.
The Disaster Event and What It Taught Us
The Disaster Incident

• Date: 8/14/18 10:20 am to 8/15/18 4:30 pm
• Situation: Regional flooding
• Provider of multiple network circuits to one data center impacted
• At 10:20 am a network provider substation carrying multiple circuits flooded
  – One data center was cut off from part of the network
  – Some branches and locations did not have email or Silverlake.
    Some locations did not have phone service.
  – Branches continued to run in offline mode and called published numbers for balances.
The Disaster Incident – August 14, 2018

Day 1

10:20 – Lost internet connectivity
10:45 – Crisis Team Meeting – Declared internal disaster
11:20 – Support ticket opened with vendor
11:20 – Status Message sent to employees Via Everbridge System
1:00 – Initiated BCP and implemented contingency procedures
1:30 – Communications to ACH
2:00 – Support case with Jack Henry
2:00 – Escalation with vendor
3:00 – Initiated back-up Fed server
5:00 – Process Teller Files
The Disaster Incident – August 15, 2018

Day 2

9:00 - Crisis Team Mtg – If problem not resolved by 2:00 Centurion declaration
9:15 - Status Message sent to employees via Everbridge System to resume contingency procedures
9:30 - Communications to ACH customers
2:00 - Update from vendor of equipment replacement & problem resolution at 4:30
4:30 - Connectivity resumes
4:30 - Catch-up work for offline activity
9:00 - EoD Processing
Lessons Learned

- When testing technology solutions during a Disaster Recovery test make sure that the backup solution to the backup solution is tested.
  - The vendor might have made changes that would have an impact.

- Test backup solutions with backup personnel to the business process key personnel.
  - Your key personnel may not be present during a disaster.
Lessons Learned

- Communicate early and often to employees.
- Document workarounds to existing processes in your BCP (COPE).
- Use your BCP during a disaster to see what critical processes need to be addressed – needed especially when key personnel are absent.
- Delegate someone to deal with the vendors' highest level of management so that operational employees can focus on restoration of services.
Lessons Learned

- Management should have key contact information of key employees / vendors / authorities with them at all times.
- Do not depend on support agencies, i.e. EMS, Police, etc.
- Anticipate key employees not being available.
- Communicate with employees / customers sooner than later.
- Provide temporary housing for key personnel and family close to recovery activity.
Lessons Learned

- Do required cross training in advance, during planning phase.
- Make it mandatory that key support employees develop a family disaster plan in advance.
- When testing technology recovery, test all technology components, simulate actual load, telcom, data requirements.
- Keep contractual requirements with recovery vendors updated.
- Be prepared for all normal communications being down, land lines, etc. Utilize texting, satellite phones, CB radios.
Lessons Learned

- When restoring multiple applications on multiple platforms, ensure that all of the data matches to a unified logical point.
- Conduct testing both at the technical level and at the business unit level.
- Get local authorities involved in testing scenarios.
- Have authorities provide education sessions or local emergency plans.
- Provide employee counseling to deal with stress, i.e. fatalities.
Evaluating Your Business Continuity Program
## Evaluate your Business Continuity Program

<table>
<thead>
<tr>
<th>Plan Elements</th>
<th>In Plan</th>
<th>Not In Plan</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency / Evacuation Plan</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Succession Plan – Escalation Plan</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alternate Work Locations Identified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Impact Analysis Conducted</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery strategies in place to restore critical functions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery Timeline Identified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical Documentation Identified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource Requirements Identified per business function</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Assessment-Risks Identified and Prioritized</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Evaluate your Business Continuity Program

<table>
<thead>
<tr>
<th>Plan Elements</th>
<th>In Plan</th>
<th>Not In Plan</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency / Evacuation Plan</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Succession Plan – Escalation Plan</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alternate Work Locations Identified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Impact Analysis Conducted</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery strategies in place to restore critical functions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery Timeline Identified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical Documentation Identified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource Requirements Identified per business function</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Assessment - Risks Identified and Prioritized</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Evaluate your Business Continuity Program

<table>
<thead>
<tr>
<th>Plan Elements</th>
<th>In Plan</th>
<th>Not In Plan</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Processing System (Software)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery Strategy / Procedures in place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Win Servers Recovery Strategies in place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telecommunication Recovery Strategies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic interface recovery strategies i.e., Internet, voice response,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vital Records Recovery Strategy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan Testing Strategy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evacuation Drills</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hot Site Test</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery Team Exercises</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan Maintenance Program in place</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Next Steps
Next Steps

- Evaluate your BCP/DR Program
- If assistance is needed, request it;
- Contact Tom for:
  - BCP Plan Reviews
  - Evaluation on what it takes to take your plan to the next level
  - BCP Mock Drill Testing
  - Demonstration of Centurion BCP Software (COPE) Centurion’s Online Planning Expert
  - Quote on Centurion BCP Services
Centurion Business Continuity Plan Development Service

**Plan Development**

- Expert consulting team
- COPE (Centurion’s Business Continuity Planning Software)
- Six month duration
- Five phase approach
- Two on-site visits
- Plan built at business unit level
- Complies with all FFIEC Guidelines on Business Continuity

**Plan Maintenance**

- 5 year term
- Updates to plan every 2 months
- On-site plan testing once per year
- Updates based on new regulatory requirement
COPE – Centurion’s Online Planning Expert
Business Continuity Planning Software Tool

• Based on Best Practices of the Financial and Business Continuity industry
• A web-based business continuity plan built on an SQL Server® platform utilizing a relational database
• Built by In-House by JHA software developers
• Fosters plan ownership at the Business Unit Level
• Access plans for planning purposes, testing, maintenance, and plan execution from any web browser
• A more effective way to manage the business continuity plan over traditional methods, i.e. Microsoft Word/Excel, Sharepoint
Gladiator Risk Mitigation Services

CoreDEFENSE

- Business Continuity
- Disaster Avoidance – Disaster Recovery
- Multilayered security to mitigate cybersecurity risk
- 24/7 security monitoring
- Provide visibility into security and controls
- Certified security and compliance staff
- Empower management oversight
- Protect your reputation

IT Regulatory Compliance
Managed IT
Hosted Network Solutions
Centurion - BC/DR
BCP/DR Support Organizations Websites

- [www.centuriondr.com](http://www.centuriondr.com)  
  - Centurion Disaster Recovery
- [www.ready.gov](http://www.ready.gov)  
  - US Department of Homeland Security
- [www.drj.com](http://www.drj.com)  
  - *Disaster Recovery Journal* (free magazine)
- [www.ffiec.gov](http://www.ffiec.gov)  
  - Federal Financial Institutions Examination Council’s site
- [www.redcross.org](http://www.redcross.org)  
  - American Red Cross
- [www.fema.gov](http://www.fema.gov)  
  - Federal Emergency Management Agency
- [www.citizenscorps.gov/cert/](http://www.citizenscorps.gov/cert/)  
  - Community Emergency Response Team
- Emergency Financial First Aid Kit – Supported by Operation Hope & FEMA
Questions?
Next in our Maturing Your Cybersecurity Program series:

Webinar 4: 
*What Can You Expect Next – Cyber Threats and Trends in 2019*

Wednesday, January 30, 2019 at 2 p.m. ET
Tom Williams
Jack Henry & Associates (Gladiator Division
Business Continuity Strategy Manager

313-318-3839 - towilliams@jackhenry.com

Susan Hubble – Debbie Dissinger – Peoples Security Bank & Trust