Disaster Recovery Planning for Mercury Processing

Thomas Aines, Client and Professional Services Manager

May 2017
PREPARE

Planning – ensuring financial services to members
Resources – allocating of sufficient equipment and facilities
Evaluation – testing contingencies for all critical systems
People – maintaining readiness of staff and officials
Alliance – establishing relationships with other organizations
Review – updating internal plans for effectiveness
Experience – incorporating lessons learned

From an NCUA News Release
“By failing to prepare, you are preparing to fail.”
— Benjamin Franklin

"Luck favors the prepared"
-- Edna Mode, The Incredibles

Organize, don't agonize.”
— Nancy Pelosi

“I believe luck is preparation meeting opportunity. If you hadn’t been prepared when the opportunity came along, you wouldn’t have been lucky.”
— Oprah Winfrey

“We are not preparing for the world we live in - we are preparing for the world we find ourselves in.”
— Michael Mabee, Prepping for a Suburban or Rural Community: Building a Civil Defense Plan for a Long-Term Catastrophe
Recovery Plan Components

- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Business Impact Analysis (BIA)
Recovery Plan Objectives

- **Principal Objectives**
  - Have an organized approach to a disruption
  - Minimize disruptions of services to the credit union and its members
  - Ensure timely resumption of operations
  - Limit loss of information
  - Limit losses to earnings and capital
  - Document and centralize important information
  - Educate your employees and other key stakeholders
• Basic plan items
  – Identify your critical information systems and business functions
  – Detail items to enable systems and functions to be continued and resumed in the event of a disruption
  – Identify responsibilities, key people, and resources
  – Develop a communication plan
  – Document and share your plan! Plan in your head does not count! A plan not shared is not a plan – it is a secret!
  – Verify that the plan compliments other Disaster Recovery plans
    • IT plans
    • Other vendors
    • Physical location
    • Transportation
    • Local government
  – Test the plan for effectiveness periodically and document the test
The FFIEC indicated that financial institutions are critically dependent on information technology (IT) to conduct business operations. ....

....[institutions need to] develop and test business continuity and disaster recovery plans that incorporate cyber incident scenarios.
Business Continuity

• Determine threats and their impact

• Risk Assessment
  – Prioritize the threats
  – Include even rare or low impact threats

• Manage the risk
  – Develop your Business Continuity Plan

• Monitor your risk

• Validate/test and update your plan
  – At least yearly
  – After major changes (IT upgrades, building moves, add a branch, new features, new risk, new employees, etc.)
  – Document the results
  – Adjust the plan from the results
  – Track changes to the plan
Business Impact Analysis

- Analyze and predict the consequences of a disruption
  - Business Impact Analysis
    - Identify critical business activities
      - Tellers, Loans, EFT processing, etc.
    - Identify critical infrastructure
      - IT systems, communications, utilities, facilities
      - Alternate location
  - Financial Impact
    - With 24 hour services
      - Yearly revenue/365
    - Without 24 hour services
      - Yearly revenue/days open
  - Determine Recovery Time Objective (RTO)
    - How long to get back up and running
    - Recovery time for the critical business activities and infrastructure
    - Be realistic
    - Account for outside assistance needed
  - Determine Recovery Point Objective (RPO)
    - How old will the data be if you need to restore?
    - How much data can you afford to lose?
      - How frequently do you backup/replicate?
      - What is your access time to your data?
Disruption Timeframes and Events

- The most common timeframes to document and test for are:
  - 1 hour
  - 4 hours
  - 1 day
  - More than 1 day
  - Total disaster

- Extended timeframe events:
  - Fire
  - Flood
  - Earthquake
  - Tornado
  - Hurricane
  - Pandemic
  - Inaccessibility to facilities
  - Cyber Attack
  - Other extreme weather
Disaster Preparedness Information

- **Pandemic**
  - [www.ncua.gov](http://www.ncua.gov)
  - [www.flu.gov](http://www.flu.gov)

- **Hurricanes**
  - [www.nhc.noaa.gov](http://www.nhc.noaa.gov)
  - [https://www.weather.gov/wrn/hurricane-preparedness](https://www.weather.gov/wrn/hurricane-preparedness)
  - Note: Hurricane preparedness week was May 7-13, 2017

- **Tornadoes**
  - [http://emergency.cdc.gov/disasters/tornadoes/](http://emergency.cdc.gov/disasters/tornadoes/)

- **Hazardous Weather in general**
  - [www.weather.gov/safetycampaign](http://www.weather.gov/safetycampaign)
  - [http://www.nws.noaa.gov/os/thunderstorm/](http://www.nws.noaa.gov/os/thunderstorm/)

- **Earthquakes**
  - [www.ready.gov](http://www.ready.gov)
  - [www.shakeout.org](http://www.shakeout.org)
    - Check the site for your state/area

- **Weather**
  - National Weather Service
    - [www.weather.gov](http://www.weather.gov)
  - The Weather Channel
    - [https://weather.com/](https://weather.com/)

- **Cyber Attack**
And of course……

- Zombie Apocalypse
  - [https://www.cdc.gov/phpr/zombies.htm](https://www.cdc.gov/phpr/zombies.htm)
Disaster Recovery Organizational Issues

• **Who is responsible for what?**
  – Defined roles with more than 1 responsible
  – Be specific about tasks and roles
  – Who speaks for the Credit Union?

• **Multiple Dependency Concerns**
  – Electricity
  – Gas
  – Oil
  – Internet
  – Facility Access
  – Personnel
  – Site Experts
  – Others?

• **Documentation**
  – Detail the action items
    - Specific “how-to’s”
    - The person executing an item may not be an expert and may need specifics
  – Contact Lists
    - Credit Union Staff
    - Board Members
    - Sponsor Company (if applicable)
    - Vendors
    - Members
    - Internet Service Provider (ISP)
    - Safeguard the information
    - Who calls who (Call Tree)
    - Local Disaster Contacts
    - Media
    - Alternate Site contacts
Disaster Recovery Organizational Issues (continued)

• Electronic contact options
  – Texting
  – Twitter account – restricted
  – Facebook – be careful of public viewables
  – Google+
  – Email
  – Skype / Facetime / Facebook Messenger
  – Cell Phones / Landlines
  – Snapchat / Kik / Whatsapp / Instagram

• Site Expert Involvement
  – Documentation
    • Including all passwords
  – Training
  – Availability

• Distribution of plan to key stakeholders
  – Hard copy
  – Electronic
  – Cloud
  – Security concerns

• Staff training on the plan

• Other stakeholder training

• What can you do to help your staff
  – Transportation
  – Authorized expenses
    • Hotel/Travel
    • Paid leave
    • Communication devices
    • Work from home
    • Other?
1. In the event of a disaster, will the credit union communicate with members through a website?
   a. Yes  b. No

2. Please check the resources or services you have available and would be willing to share with other credit unions during the time of an emergency if you did not need them. (Check all that apply)
   a. Cash Non-Member Share Drafts  c. IT Support  e. Office Space
   b. Generator  d. Mobile Branch  f. Staff/Management Services

3. Please provide the date of the last disaster recovery test completed by the credit union ____________
   a. Indicate the method(s) used for the last disaster recovery test completed by the credit union.
      2. Tabletop/Mini-Drill  4. Full-Scale Testing
Mercury Information
Data Backups

• **Mercury**
  - Backups include transactions, settings, and history
  - Mercury can be backed up anytime
    - Manually
    - Mercury Scheduler
    - MercuryOnDemand is backed up every night as well as replication to the disaster recovery site
  - 2 SQL Backup files – CU and Common
    - Overwrite versus Append
  - BankTel and/or SmartCOLLECTOR
  - MDS (Mercury Data Solutions) [optional]

• **Network**
  - Consult your Site Expert

• **How often should you backup?**
  - Daily
    - Could be 24 hours behind
    - Skip weekends? 48 to 72 hours behind
    - Holidays? 6 3-day weekends in 2017

• **Verify your backups**
  - Restore backups and test your DR server
  - Have FIS verify a backup for you (Backup Verification)

• **What else should you backup?**
  - Disaster Recovery Plan
    - Make sure to include any attachment documents
  - Custom programs
  - EFT files
  - Images
  - Loan forms / Rate files
  - Credit Union Documents
  - Critical Non-Mercury information
Backup Storage & Media

- **“Cloud” storage***
  - Preferred for sending data offsite versus physical media
  - Verify the security on the site and the physical location
  - Should be a secure transfer method
    - HTTPS or Secure FTP

- **DVD/CD***

- **USB/Jump drives***
  - Some have encryption software on them
    - Store safely

- **Tapes***
  - Tapes require specific software and hardware to restore

- Review who you are storing with
  - Is it an established company?
  - Are they audited? SSAE16
  - Are the compliant for your type of data? (PCI, NPI, etc.)
  - Review their security
  - Is the datacenter far enough away that it makes sense?
  - What is the availability of your data?
  - Do they have 24/7 support?

  - Username tracking
  - Password rotation
  - Remove employees that leave
  - Add/Remove employee access when roles change
  - Add new employee access as appropriate

*files should be encrypted or at least password protected
In-house Clients Disaster Recovery Server

• Software to install
  – Microsoft SQL (compatible to your in-house version)
  – Anti-virus software
  – Mercury
    • Follow the normal Mercury installation instructions and install all the parts you need
      – Mercury (keep your versions updated)
        • Prereqs/Workstation/Server
      – Mercury Reports
      – Application Manager
      – Scheduler
      – Gateway
      – Digital Dialogue
      – Mercury Data Solutions (MDS)
  • Other critical software
    – MS Office or Open Office software
    – 3rd party EFT programs

• Information to copy
  – Loan document files
  – Rate files
  – Custom Programs (EFT, CPI Exports, MDS Excel Sheets)
  – Images (photos, ID)
  – Important documentation
    • Credit Union policies and procedures
  – Business Continuity Plan
    • Remember the attachments

• Other items
  – Checks
  – Paper
  – Receipts
  – Printer(s)
  – VPN
MercuryOnDemand Disaster Recovery Machine

• Laptop or Desktop
  – Wireless and hard wired network connection capable
  – Extended Network cable
  – Power supply
  – Mouse (or other pointing device)
  – Keyboard
  – Monitor (for a desktop)

• Internet access

• FIS Software VPN client

• Other Software
  – 3rd party EFT programs (if not on your MOD server)
  – MS Office or Open Office software
  – Anti-virus software
  – Filezilla

• Business Continuity Plan
  – Remember the attachments

• Important Documents
  – Credit Union policies and procedures
  – Copies or online access to important files
In-house or MercuryOnDemand DR (continued)

- **Critical website list**
  - Copy of your important bookmarks (Export, save a copy)
  - NCUA [www.ncua.gov](http://www.ncua.gov)
  - Federal Emergency Management Agency (FEMA) [www.fema.gov](http://www.fema.gov)
  - Financial Services Information Sharing and Analysis Center (FS-ISAC) [www.fsisac.com](http://www.fsisac.com)
  - Your Credit Union league
  - Center for Disease Control and Prevention [www.cdc.gov](http://www.cdc.gov)
  - Local TV stations and newspapers
  - Local Organizations that coordinate in your area
  - Red Cross [www.redcross.org](http://www.redcross.org)
  - FIS Client Portal [clientsupport.fisglobal.com](http://clientsupport.fisglobal.com)
    - Mercury >> Help >> FIS Client Portal
  - FIS Mercury [www.mercurydelivers.com](http://www.mercurydelivers.com)
    - Mercury >> Help >> Mercury on the Web
Pandemic Example
Flu Statistics

• Only approximately two of every five children and adults in the United States were vaccinated by early November 2016:
  – 39.8% of all persons 6 months and older
  – 37.3% of children 6 months through 17 years
  – 40.6% of adults 18 years and older

• As of the 2014-2015 season, the CDC reports that about 44% of adults and 60% of children in the United States have been vaccinated.

• March 2017 According to data from the U.S. Flu Vaccine Effectiveness Network, interim estimates show flu vaccine has been 48% effective.
  – In January 2016 the CDC reports this season’s vaccine is nearly 60% effective.
  – In January of 2015 the CDC reported that flu shots were only 23% effective.
Pandemic Example

- **Day 1**
  - The news reports some cases of flu in your area hospitals
  - One of your employees knows someone with symptoms

- **Day 2**
  - The news reports several in the hospital died
  - New cases have been reported in 2 local schools
  - 1 employee calls in sick

- **Day 3**
  - You or people you work with know someone who has flu
  - Several local schools are closed
  - 2 employees do not come to work, 1 reports symptoms
Pandemic Example (continued)

- **Day 4**
  - More schools are closed
  - More deaths are reported from local hospitals
  - 25% of your employees do not come to work (call in)
  - Another 25% cannot be contacted
  - Fewer members are coming to the CU, phone calls increase
  - ATM/Debit card activity increases
  - Home Banking and Mobile Banking activity increases

- **Day 5**
  - All schools are closed on your area
  - Public gatherings are discouraged
  - 4 members of your Board and Supervisory Committee report symptoms or are sick
  - The Manager/CEO report symptoms
  - Only 10% of your staff is willing to come to work
  - Your sponsor company or building owner closes your facility
Pandemic Example (continued)

• Day 6
  – More deaths are reported
  – Travel in/out of your city is restricted
  – Communication channels are clogged

• Day 20
  – The illness has subsided and you can return to your building to work and your members are able to come to your facility
  – Only 50% of your staff returns to work
Cyber Attack Example
Cyber Attack Example

- Your internet stops responding or is extremely slow
- Cards are being declined
- Online and Mobile Banking is not responding with new information
- Shared Branching is not responding
- You are not able to send or receive email
Cyber Attack Example (continued)

• After several hours, it is discovered that you are the victim of a Distributed Denial of Service (DDos) attack
  – an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources

• By the next day your ISP is able to block the traffic bombarding your internet router

• Internet, online services and email return to normal

• Possible defenses
  – Have a secondary internet connection
  – Run credit union services through a separate connection from general internet
  – Monitoring on your internet routers
  – Determine what your ISP can do in these situations and what YOU need to do to get their help
  • Document the process
FIS Offerings

• Web Vault/Evault
  – Secure Electronic Data Storage
  – Secure Transfer
  – 24/7 access
  – FileMover option for secure automated uploads
  – Password rotation

• Rapid Recovery
  – Access to a limited environment via FIS managed hardware or software VPN
  – Environment is based on the MercuryOnDemand (MOD) model

• Disaster Recovery Audit
  – Onsite or phone assistance to create, document, train and test a Disaster Recovery Plan
  – An optional Annual Review and Update of the plan is available
• **Backup Verification**
  – Verification that your data can be restored
  – Set of pre-defined reports of your choice returned to you electronically
  – Letter from FIS stating what was done

• **Software VPN with secure token**
  – For in-house, if you have an FIS Fortigate VPN device you can connect to your system remotely (note: may require other setup coordinated with your site expert)
  – For MercuryOnDemand, can be used to connect directly to your system in Charlotte
  – Can be used for disaster recovery, remote branch, membership events, loan events, etc.

• **Mercury On Demand (MOD)**
  – Hosted environment on remote server in Charlotte, NC
  – Same Mercury software
  – Secure connection via FIS managed VPN (sw or hw)
  – Online services run to Charlotte so issues at your local office do not impact member access
  – Uses Microsoft Remote Desktop to connect so only minimal workstation hardware is required
  – Mercury upgrades and patches are done for you
  – Mercury backups and data replication are done
Our Disaster Recovery Plan Goes Something Like This...
DO, OR DO NOT...
THERE IS NO TRY

-YODA
BE PREPARED
Thank You

Thomas Aines
thomas.aines@fisglobal.com

T: 800.998.4357 x9
O: 501.407.5120
C: 801.232.3128