Business Continuity and Disaster Recovery

CROGHAN
COLONIAL BANK

EQUAL HOUSING LENDER • MEMBER FDIC

Natural Disaster Presenter

CROGHAN
COLONIAL BANK

EQUAL HOUSING LENDER • MEMBER FDIC

Melissa Walker

VP, Retail Operations and Security

Digital Disaster Presenter

CROGHAN
COLONIAL BANK

EQUAL HOUSING LENDER • MEMBER FDIC

Jacob Molyet

Information Systems Officer

Disaster Recovery Presenter

CROGHAN
COLONIAL BANK

EQUAL HOUSING LENDER • MEMBER FDIC

Carla Waggoner

SVP, Chief Operating Officer

Human Disaster Presenter

CROGHAN
COLONIAL BANK

EQUAL HOUSING LENDER • MEMBER FDIC

Shantel Laird

AVP, Senior Commercial Deposit Officer

Break Out Session

- Each table will be given a disaster scenario
  - Digital Disaster
  - Human Induced Disaster
  - Natural Disaster

- Take 10 minutes to complete your responses to the Business Continuity and Disaster Recovery (BCDR) sheet

Break Out Session

CROGHAN COLONIAL BANK

Helping good people make good decisions.

A Semi Has Entered The Building

CROGHAN COLONIAL BANK

Helping good people make good decisions.

Complete Service Interruption

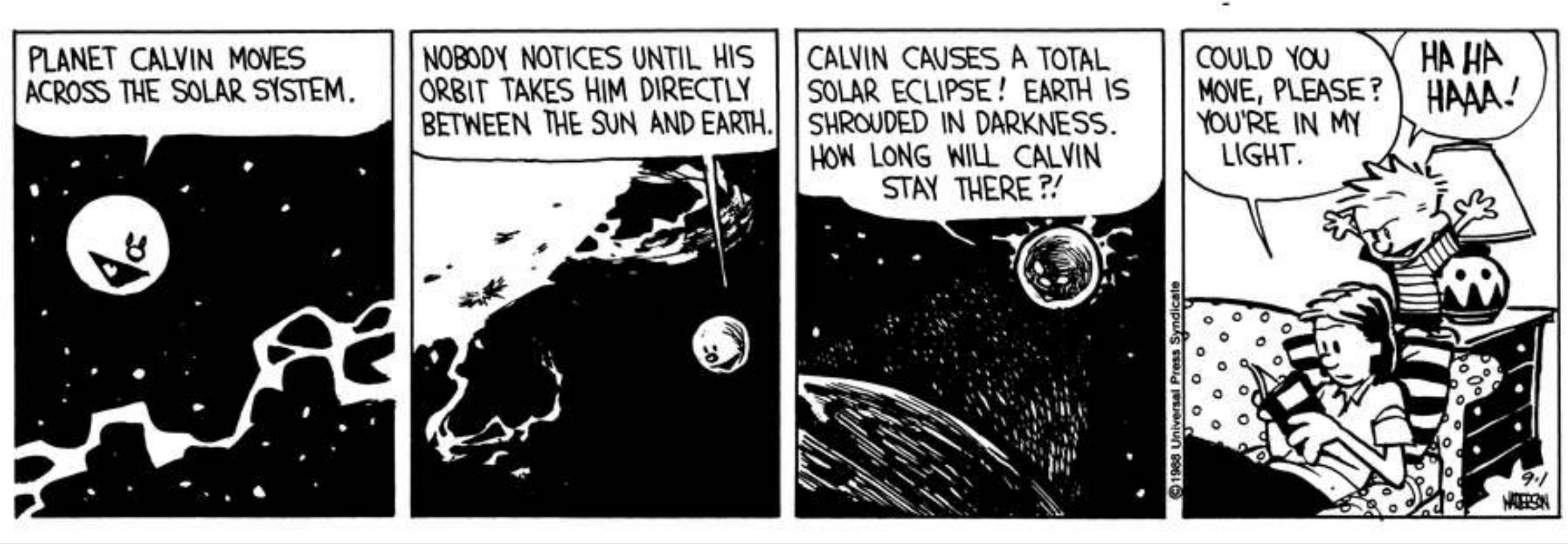
- **Incident Summary**
- **Impact**
- **Business Continuity**
  - Who to Report Incident to
  - Plan for Temporary Closure
  - Impact to Lack of Access for Municipality
  - Plan for Customer Impact
  - Emotional/Security Employee Impact
- **Disaster Recovery**
  - Plan and Agreements in Place for:
    - *Quick restoration of services or back up access*
    - *Physically repair the building to secure it or consider security staff.*
- **Mitigation**
  - Height Sign

Practical Joke Gone Wrong

Partial Service Interruption

- **Incident Summary**
- **Impact**
- **Business Continuity**
  - Who to Report Incident to
  - Plan for Temporary Closure
  - Impact to Lack of Access
  - Plan for Customer Impact
  - Health and Safety of Employees
  - Legal Action
- **Disaster Recovery**
  - Plan in Place for:
    - *Public Health Procedures*
    - *Sanitization*
- **Mitigation**
  - What's Practical?

Blinded by The Light

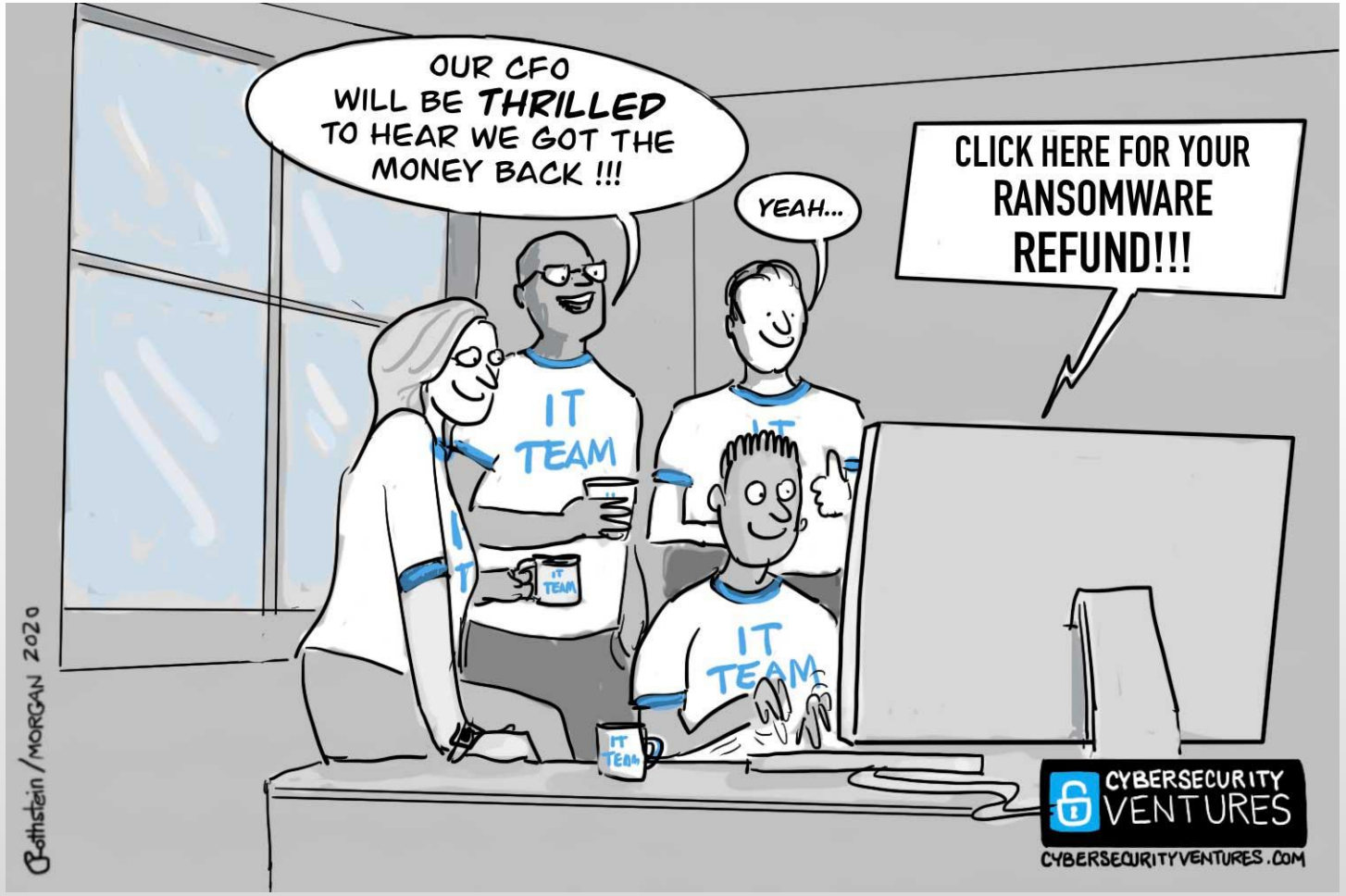


Service Interruption

- **Advantages**
  - Exact time and date known
  - 2017 Lessons Learned from EMA
- **Impact**
  - Expected
  - Potential
  - Other-Employee
- **Business Continuity**
  - Who to Report Incident to
  - Plan for Temporary Closure
  - Impact to Lack of Access
  - Plan for Customer Impact

- **Disaster Recovery**
  - Plan in Place for:
    - *Lack of Internet or Phone Service*
    - *Staffing*
    - *Educate and Empower Managers and Employees*
- **Mitigation**
  - EMA Resources
  - Tabletop exercise to develop plan
  - Customer Advanced Notice and Communication
  - Train Staff
  - Educate other Business' for preparation

Payment Due Now



Government Ransomware

- **Incident Summary**
  - City infrastructure was compromised and data was encrypted
- **Impact**
  - Can effect everything – Tax, Zoning, Utilities, Engineering
  - Potential Unauthorized Access
  - Potential Further Impersonation
- **Business Continuity**
  - Who to Report Incident to
  - Plan for offline work
  - Notify effected users
- **Disaster Recovery**
  - Plan in Place for:
    - *Ransomware*
    - *Authorized Access*
    - *Extended Offline Procedures*
- **Mitigation**
  - Phishing Training
  - Data Backups
  - Air Gap

School Ransomware

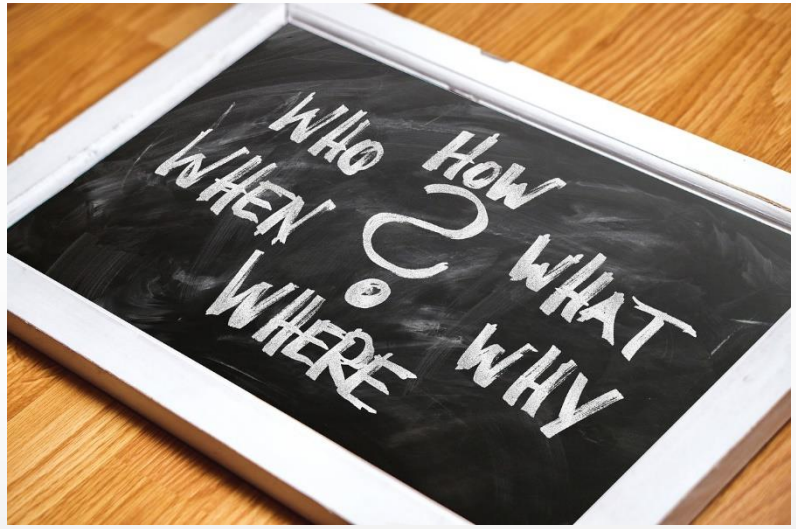
- **Incident Summary**
  - Clicked a compromised link and data was encrypted
- **Impact**
  - Accounts Payable, SIS, Transportation
  - Teaching impacts
  - Potential Unauthorized Access
- **Business Continuity**
  - Who to Report Incident to
  - Plan for offline work
  - Notify effected users
- **Disaster Recovery**
  - Plan in Place for:
    - *Ransomware*
    - *Authorized Access*
    - *Extended Offline Procedures*
- **Mitigation**
  - Phishing Training
  - Data Backups
  - Air Gap

By the Numbers

- **In Ohio**
  - Public governments have been a target and Ohio has seen local governments exploited in 2023
- **In Education Sector**
  - The White House and the U.S. Department of Education last month hosted the "Cybersecurity Summit for K-12 Schools" after the 2022 school year became the fourth year in a row with more **than 50 ransomware attacks**, including four that forced schools to cancel classes.
- **Several Schools in Ohio have been hit in the last 12 months**
- **Social Engineering**
  - *What is it and Why is it so Common*
- **Phishing**
  - *Getting harder and harder to spot the differences between real and fake with AI*

Additional Mitigation Steps

- **Train, Train, Train**
  - *Monthly Phishing Test*
  - *Annual Training*
- **Data Backup Plan**
  - *How Often are You Backing Up*
- **Air Gap Solution**
  - *Off Network Version of Your Data*
- **Strong Permissions**
- **Containment Software**
- **Antivirus**



We're Prepared

Disaster Recovery Session Outcomes

- Understand the importance of Business Continuity/Disaster Recovery (BCDR) planning and preparation.
- Understand the unique challenges of responding to a disaster.
- Identify important keys to effective recovery operations.
- Strengthen your personal capability to conduct a BCDR project.

Importance of BCDR

Disaster Recovery vs. Business Continuity

- BCDR is a set of closely related practices that support an organization's ability to remain operational after an adverse event.
  - Business Continuity is a business's level of readiness to maintain critical functions after an emergency or disruption.
  - Disaster Recovery is the process of maintaining or reestablishing vital infrastructure and systems following a natural or human-induced disaster.

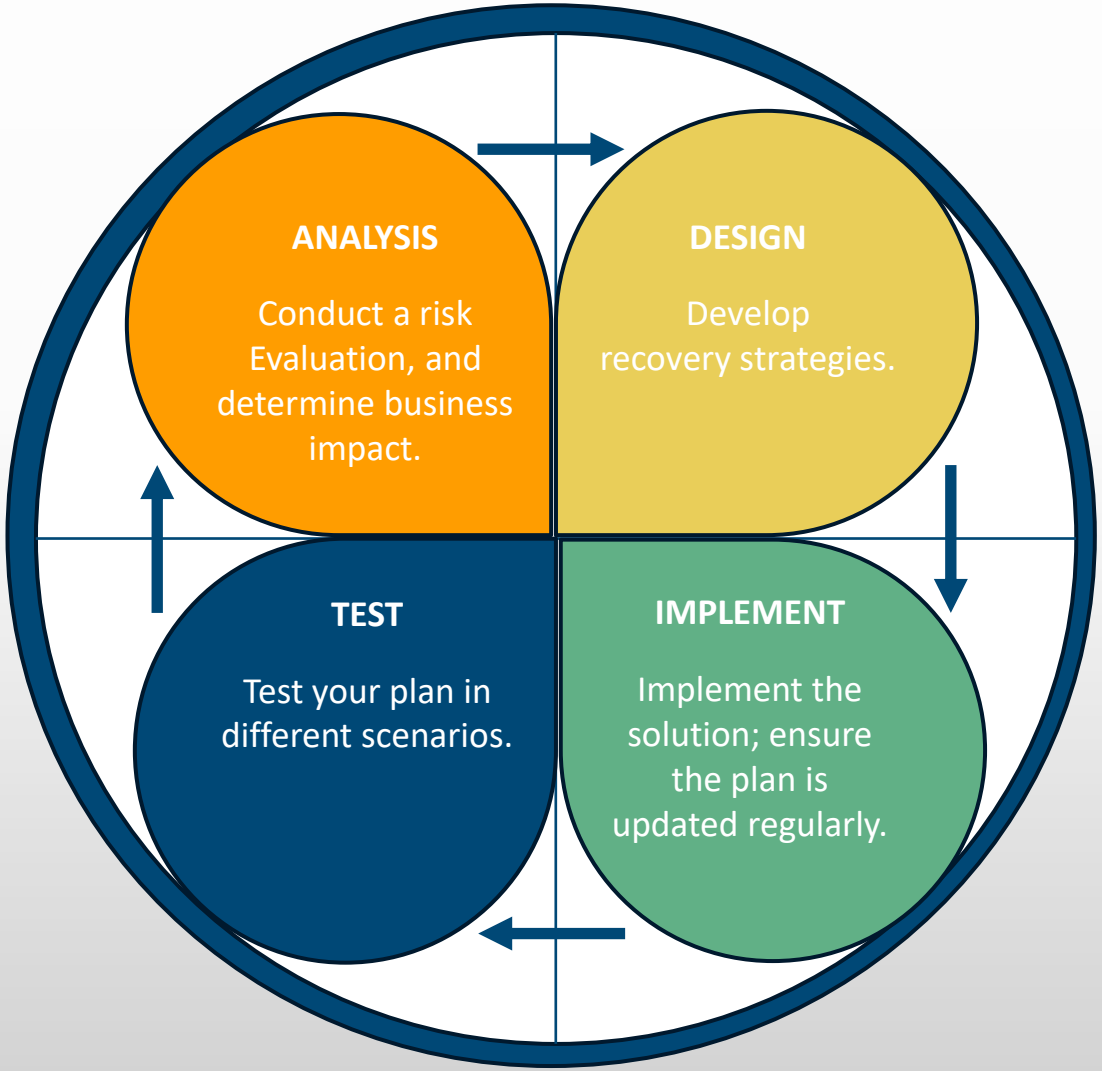
Why BCDR?

- Ensure Business Resilience
- Safety of
  - Employees
  - Visitors
  - Customers
- Mitigate Financial Loss
- Maintain Competitiveness and Reputation
- Mitigate Data Loss and Productivity
- Continue to Provide Great Customer Service

Challenges of BCDR

- Fractured Command and Control Structures
- Ineffective Communication
- Delayed or Inefficient Deployment of Resources

A Glance at Business Continuity



CROGHAN COLONIAL BANK
Helping good people make good decisions.

A Glance at Disaster Recovery

6 Steps to a Successful DRP

1. Identify Critical Infrastructure and Services
2. Conduct a Risk Assessment
3. Determine Disaster Recovery Objectives
4. Create Written Policies and Documentation
5. Test, Revise, and Adapt
6. Regularly Update Your Disaster Recovery Plan

Step 1

Identify Critical Infrastructure and Services

- An organization must comprehensively understand its infrastructure and the services it supports before designing disaster recovery processes.
- Assign roles and responsibilities.
- An infrastructure inventory is often one of the most time-consuming aspects of disaster recovery planning, but it is necessary.

Step 2

RISK ASSESSMENT MATRIX TEMPLATE

RISK RATING KEY	LOW	MEDIUM	HIGH	EXTREME
	0 – ACCEPTABLE OK TO PROCEED	1 – ALARP (as low as reasonably practicable) TAKE MITIGATION EFFORTS	2 – GENERALLY UNACCEPTABLE SEEK SUPPORT	3 – INTOLERABLE PLACE EVENT ON HOLD

	SEVERITY			
	ACCEPTABLE LITTLE TO NO EFFECT ON EVENT	TOLERABLE EFFECTS ARE FELT, BUT NOT CRITICAL TO OUTCOME	UNDESIRABLE SERIOUS IMPACT TO THE COURSE OF ACTION AND OUTCOME	INTOLERABLE COULD RESULT IN DISASTER
LIKELIHOOD				
IMPROBABLE RISK IS UNLIKELY TO OCCUR	LOW – 1 –	MEDIUM – 4 –	MEDIUM – 6 –	HIGH – 10 –
POSSIBLE RISK WILL LIKELY OCCUR	LOW – 2 –	MEDIUM – 5 –	HIGH – 8 –	EXTREME – 11 –
PROBABLE RISK WILL OCCUR	MEDIUM – 3 –	HIGH – 7 –	HIGH – 9 –	EXTREME – 12 –

Conduct a Risk Assessment

- A risk assessment documents and prioritizes risks to a business's operations.

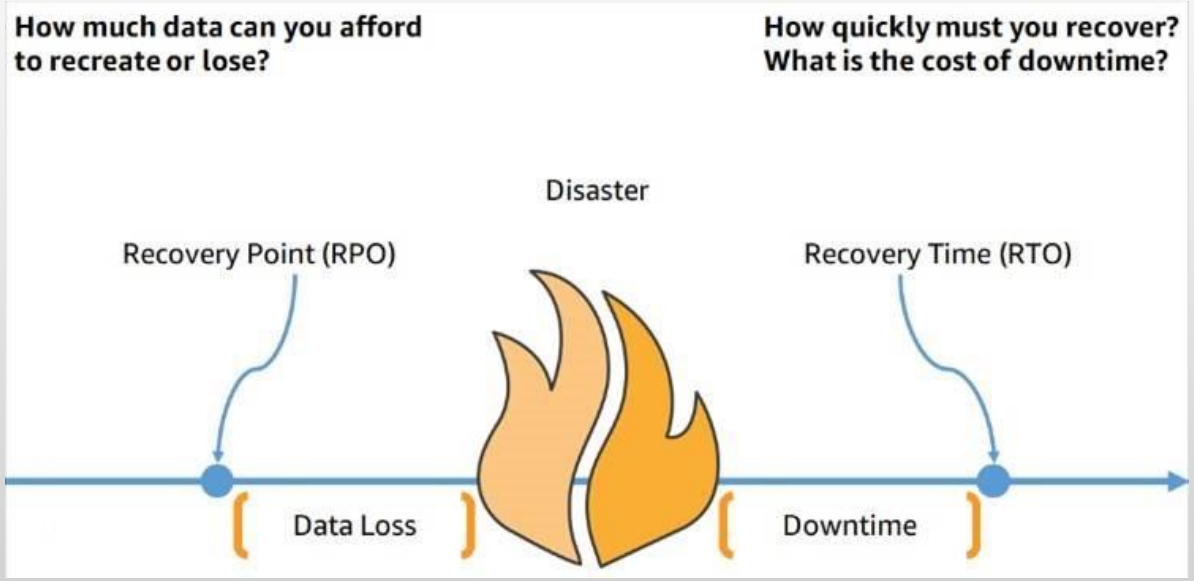
CROGHAN COLONIAL BANK

Helping good people make good decisions.

Step 3

Determine Disaster Recovery Objectives

- The next step is to prioritize systems and determine your disaster recovery objectives.
- Objectives are usually expressed as Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).



Step 4

Create Written Policies and Documentation

- At this point, you understand your IT infrastructure's risks, how to prioritize disaster recovery planning, and your disaster recovery objectives.
- The next step is to create disaster recovery policies to achieve those objectives.

Step 5

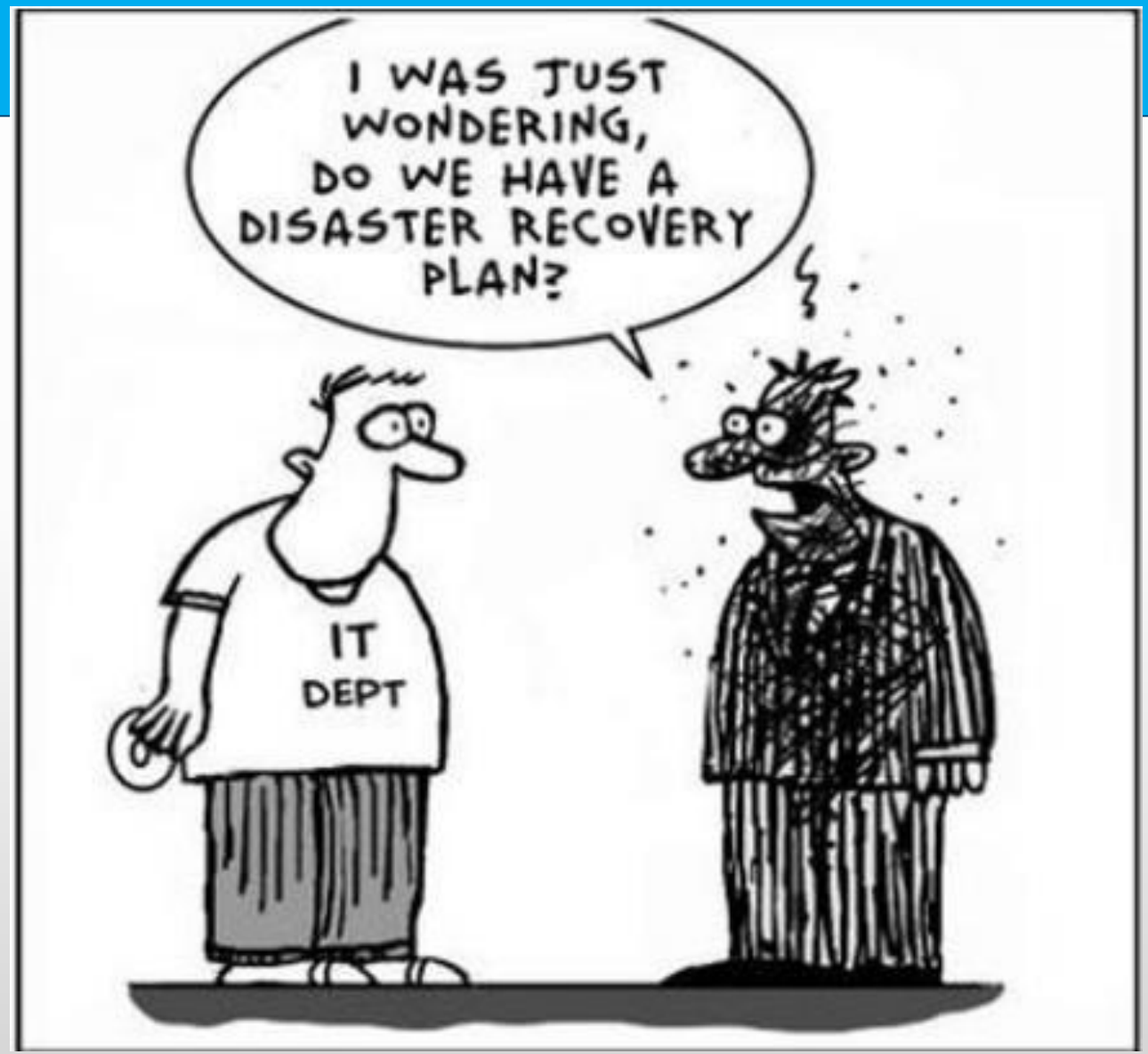
Test, Revise, and Adapt

- Once your disaster recovery plan is in place, it should be tested to make sure it survives within the real world.

Step 6

Regularly Update Your Disaster Recovery Plan

- Your company's IT infrastructure and processes evolve, and your disaster recovery plan should evolve with them. DR planning is not a "once and you're done" event.
- Businesses must iterate on their plan continuously, ensuring that policies and documentation reflect current systems and priorities.



Break Out Session

- Revisit your Tables Disaster Scenario
  - Digital Disaster
  - Human Induced Disaster
  - Natural Disaster

- Take 10 minutes to note how you'd revise your previous responses to the BCDR sheet

Questions

CROGHAN COLONIAL BANK

Helping good people make good decisions.

Takeaway

- **Tabletop Exercise Toolkits**
  - Tabletop Exercises are discussion-based exercises intended to stimulate dialogue of various issues regarding a hypothetical situation. Tabletop exercises can be used to assess plans, policies and procedures, or to assess types of systems needed to guide the prevention of, response to, or recovery from a defined incident.
  - Tabletop Exercise Toolkits provide all of the materials, information and resources needed to plan and host an effective tabletop exercise.

Scan the QR Code to View these Examples

CROGHAN COLONIAL BANK

Helping good people make good decisions.

Thank You

CROGHAN
COLONIAL BANK

EQUAL HOUSING LENDER • MEMBER FDIC