The webcast will start at 1 p.m. Eastern

Please note:

- Handout – You can print or download the webcast handout at capincrouse.com/webcast-disaster-recovery
- CPE – CPE certificates will be emailed to you within the next few weeks. To receive CPE credit you must respond to the polling questions, which are not available on mobile devices. Therefore, in order to receive CPE credit you must log in via a computer.
- Recording – A recording of today's webcast will be available at capincrouse.com/webcast-disaster-recovery

Overview

- Introduction
- Disaster plans
- Disaster testing
- Disaster training

Introduction

TRAINA & ASSOCIATES
A CAPINCROUSE COMPANY

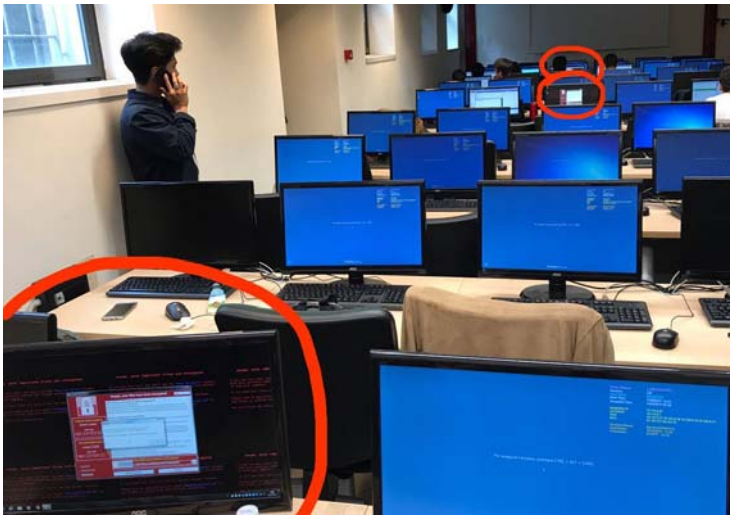
Types of Disasters

Types of Disasters

Types of Disasters

Types of Disasters

Types of Disasters



Types of Disasters

- Weather events
- Cybersecurity issues (breaches)
- System failures
- Vendor failures
- Civil unrest
- Terrorism
- Pandemics

Disaster Recovery (DR) Statistics

- Nearly 40% of small businesses close after a disaster (FEMA)
- 52% of businesses indicate 3 months needed to re-open
- Only 29% that re-open are in business after 2 years
- IT down for more than 9 days = bankruptcy

DR Statistics

- One hour of down time = $8,000 (small business) to $700,000 (large enterprise)
- More than 50% of businesses do not have adequate DR
- 45% down time is operational, 35% natural disasters, 19% human error

Operational

- July 2016
- 12-hour outage caused by router issue
- 2,300 flights canceled from Wednesday – Sunday
- 11% of flights impacted
- 33.6% decline in quarterly profit

Human Error

- February 2017
- Employee debugging an issue caused 5-hour outage
- Amazon S3 is used by over 148,000 websites, including Expedia and U.S. Securities and Exchange Commission
- Connected lightbulbs, thermostats, and other IoT hardware impacted

Mother Nature – Mississippi River Floods

- May – June 2011
- Approximately 400 deaths
- $4 billion damage
- Mississippi, Tennessee, Arkansas, Illinois, Kentucky, Louisiana

Mother Nature – Great Tri-State Tornado

- March 1925
- Approximately 700 deaths
- 219-mile track
- $1.4 billion damage
- Missouri, Illinois, Indiana

Mother Nature – Hurricane Katrina

- August 2005
- Approximately 1,800 deaths
- $108 billion damage
- Florida, Louisiana, Mississippi, Bahamas, Alabama, Cuba, eastern North America

Never Say Never

Disaster Planning

TRAINA & ASSOCIATES
A CAPINCROUSE COMPANY

Plan Objectives

- Protection of personnel
- Protection of property and records
- Continuity of management
- Restoration of critical, essential, and non-essential functions

First Steps

- Perform a risk assessment
  - What is YOUR greatest area of risk?
  - Consider the potential for area-wide disasters that could affect an entire region and result in significant losses
  - Factor in lessons learned from past disasters
- Perform a business impact analysis

YOUR Greatest Risks

Does your business…

- Rely on a single location?
- Rely on a service provider?
- Have geographically dispersed resources?
- Rely heavily on manpower? Computer systems?

One size does NOT fit all!

Assessing Risks

- Assess vulnerabilities
  - Internal and external threats
  - Estimate likelihood
  - Consider potential impact on employees and customers, property, and business operations
  - Assess internal and external resources available

Assessing Risks

Scenario	Probability	Potential Impact
Natural Causes		
Air contaminants or hazardous spills	Low	Low
Earthquake	Very Low	Medium
Epidemic or pandemic	Low	High
Fire	Low	High
Flood	Medium	High
Hurricane	High	High
Other severe weather	High	Low
Tornado	Low	High
Human Threats & Malicious Activity		
Arson	Low	High
Bombing	Low	High
Civil strife	Low	Low
Fraud, theft or blackmail	Low	Medium
Human Error	Medium	Medium
Terrorism	Low	High
Vandalism	Low	Medium
Technical Threats		
Communications failure	Low	High
Data or systems destruction and corruption	High	High
External intrusion/attack (e.g., zero-day attacks, DoS/DDoS attacks)	High	High
Hardware or software failure	High	High
Insider threats (e.g., disgruntled employee targets production data or backups with intent to destroy or corrupt)	Low	High
Malware	High	High
Power failure	High	Medium
Vendor failure	Low	High

YOUR Plan

- Based on the **size and complexity** of your organization
- Consistent with your organization's **overall business strategy**
- Aim to **minimize financial losses** to the organization, **serve customers** with minimal disruptions, and **mitigate the negative effects** of disruptions on business operations

Plan Details

- Business Impact Analysis (BIA)
  - Determine critical functions
  - Estimate maximum downtime
  - Evaluate resource requirements

BIA

- Consider the following in defining critical support areas and interdependencies:
  - Telecommunications
  - IT departments
  - Transportation and delivery services
  - Shared physical facilities, equipment, hardware, and software

BIA

- Consider the following in defining critical support areas and interdependencies (cont'd):
  - Third-party vendors
  - Back-office operations, including accounting, payroll, transaction processing, customer service, and purchasing

Plan Details

- Succession plans
- Emergency team assignments
  - DR Coordinator
  - DR Team
- Functional areas and team members
  - Critical (24 hours), essential (1 week) and non-essential functions

Plan Details

- Disaster declaration
- Alternate locations
- Records protection
- Media relations
- Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
- Pandemic plan

Emergency Procedures

- Evacuation
- Shutdown, recovery, restart
- Functional area procedures
- IT procedures
- Location recovery
- Re-entry requirements

Reference Information (Appendices)

- Emergency team contact lists
- Vendor, local government agencies, business contacts
- Employee communications procedures/contact info

Reference Information (Appendices)

- Summary of insurance
- Listing of off-site supplies
- Inventories
- Telecomm circuit info
- Temporary closing sign

Get Involved in Planning BEFORE a Disaster

- Establish an **ongoing relationship** with **community and government officials** and the **news media** to ensure the successful implementation of the Plan

Disaster Testing

TRAINA & ASSOCIATES
A CAPINCROUSE COMPANY

Disaster Testing

- Annual
- As major changes are implemented
- All locations, if feasible
- IT, critical functional areas, Third-party Service Providers (TSP)

Testing Methods

- Planned and scheduled tests
- Unplanned, 'live' tests
- Tabletop testing

Testing Scenarios

- TSP outage or disruption
- Organization outage or disruption
- Cyber events

Testing Complexity

- Multiple systems
  - External dependencies
- Inter-dependencies
- End-to-end testing
- Full-scale (including TSP)
- Include TSP's subcontractors and vendors

Testing with TSPs

- Annual DR test
- Consider capacity issues
- Evaluate test results
- Obtain DR test documentation

Testing Organization Outage

- Loss of systems
  - Test restore
  - Vendor reliance
  - Failover servers
- Loss of communications
  - Test backup Internet, Wide Area Network

Testing Organization Outage

- Loss of power
  - Test generator
- Loss of facility
  - Test backup site, co-location
- Loss of personnel
  - Test with skeleton staff

Testing Cyber Events

- Malware
- Insider threats
- Data/systems destruction or corruption
- Communications disruption
- Simultaneous attack on TSP and Organization

Post-testing

- Document results
- Correct identified issues
- Modify DR Plan as needed
- Schedule re-test, if needed

Disaster Training

TRAINA & ASSOCIATES
A CAPINCROUSE COMPANY

High-Level DR Plan

- All employees
- Annually
- Document content

High-Level DR Plan

- Executive succession
- Alternate locations
- Communications procedures
- Team membership

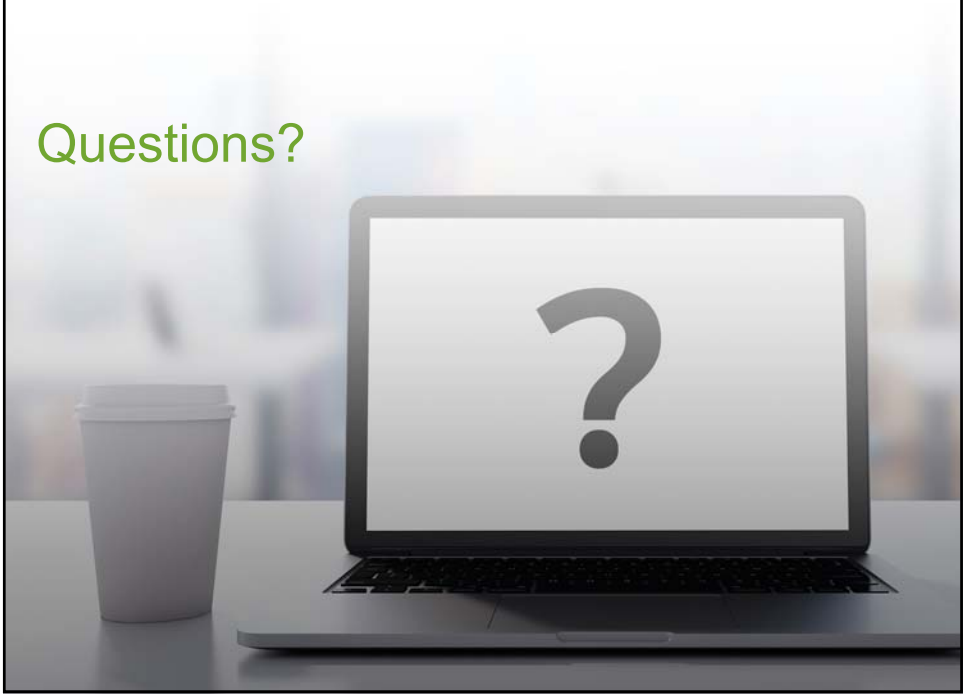
High-Level DR Plan

- Return to work expectations
- Re-entry requirements
- Pandemic plans

Functional Area Training

- Job-specific, documented procedures
- Cross-training/job swapping
- Tabletop/scenario-based
- Supplies needed
- Prioritize critical, essential, non-essential
- Document!

Questions?



Upcoming Webcast

Please join us! Learn more at capincrouse.com

Simplifying Implementation of FASB ASU 2016-14
February 28, 2019
1 p.m. Eastern
Presented by: Chris Gordon and Ruth Granlund

Thank you.

Holly G. Boullion, Principal
Traina & Associates

cybersecurity@capincrouse.com
225.308.1712

TRAINA & ASSOCIATES
A CAPINCROUSE COMPANY