WOLF
& COMPANY, P.C.

How Healthcare Providers and Life Science Organizations Can Take BCP to the Next Level

April 9, 2019

About Wolf & Company, P.C.

- Established in 1911
- Offers Audit, Tax, and Risk Management services
- Offices located in:
  - Boston, Massachusetts
  - Springfield, Massachusetts
  - Albany, New York
  - Livingston, NJ
- Over 300 professionals

Presenters

Tracy L. Hall, MBCP
IT Assurance Manager
Wolf & Company, P.C
Direct: (413) 726-6884
thall@wolfandco.com

Michael E. Kanarellis, HITRUST CCSFP
Principal
Director Healthcare IT Audit & Security Practice
Wolf & Company, P.C.
Direct: (617) 428-5408
mkanarellis@wolfandco.com

Today's Agenda

- Healthcare Regulatory Landscape
- Why Business Continuity Planning (BCP)?
- Current BCP Hot Topics
- Q & A

Healthcare Regulatory Landscape

Cyber breaches are a big concern right now!

In 2018, healthcare was the most compromised sector.

- **374** - total reported healthcare breaches
- **5.1 million** - patient records impacted
- **28%** - percentage of total breaches across all sectors
- **7.35M** - Average cost of a breach per organization
- **$380** - Per record cost ($141 per record across all sectors)

Whether a cyber attack results in a breach or not, they can be responsible for taking systems offline which results in activation of a BCP/DR Plan.

2018 Cost of Data Breach Study; Ponemon Institute

Regulatory Landscape; WannaCry

- Targeted known vulnerability in Windows OS
- Hundreds of thousands of computers encrypted in several days
- Healthcare organizations worldwide experienced service interruptions
  - Medical devices hit especially hard
- Damage due to downtime and remediation efforts
  - A strong Business Continuity Plan is the best way to mitigate the risk of Ransomware

Downtime in Health Care…

2014 study led by Dean Sittig, PhD, a professor at the University of Texas Health's School of Biomedical Informatics. Dr. Sittig's team found nearly all (96 percent) of the 50 large, integrated institutions surveyed experienced at least one unplanned system downtime in the previous three years.

Health care institutions can lose an estimated $1M PER DAY if critical systems are offline.

Downtime in Health Care…

- A major health care company out of CA was down for more than 24 hours in early 2018
- Resorted to paper record keeping
- Outage caused by a faulty fire suppression system in the data center

Regulatory Landscape; HIPAA/CMS

- Contingency Plan Standard; 164.308(a)(7)
  - Data Backup plan
  - Disaster Recovery plan
  - Emergency Mode Operation Plan
  - Testing and Revision Procedures
  - Application and Data Criticality Analysis

Regulatory Landscape; OCR

Violation Category	Each Violation	All Identical Violations per Calendar Year
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect – corrected in 30 days	$10,000 - $50,000	$1,500,000
Willful Neglect – not corrected	$50,000	$1,500,000

The Importance Of BCP

- A recent survey showed that the top causes of downtime were: (note that percentages may be combined)
  - UPS or Hardware Failure 55%
  - Human Error 48%
  - Cyber Attack 34%
  - Software Failure 18%
  - Natural Disasters 4%

- *Downtime estimates at $7,900 per minute*
- *A study comprised of 41 benchmarked data centers found the average costs of unplanned data center outages include more than $179K in business disruption, a little over $118K in lost revenue and approximately $42K in IT staff productivity*

The Importance Of BCP

- Don’t Let The Door Hit You…
  - 93% of businesses that experience downtime of 10 days or more file bankruptcy within one year
  - 40% of business severely compromised by a disaster go out of business within 6 months

BCP Process

- Business Impact Analysis (BIA)
  - Functions
  - Resource Requirements
  - Business vs. IT Gap Assessment
- Risk Assessment
- Plan Development
  - Introduction
  - Executive Oversight
  - Scope
  - Assumptions
  - Teams/Roles
  - Recovery Strategy

Business Impact Analysis

Business Impact Analysis (BIA)

The process of identifying and prioritizing critical business functions and the resources required to support them into predefined RTOs. Determining RPOs for systems. Should be BUSINESS driven, not IT driven.

This exercise is considered **POST** outage.

- Business Functions
- Departments
- Technologies

Risk Assessment

Risk Assessment

The process of identifying the **probability** of specific threats affecting the organization and the **impact** on the organization if they were to occur.

This exercise is considered **PRE** outage.

- Threat Assessment
- Control Assessment

Scenario Based Planning

Worst Case:

Identification of Worst Case type scenario with consideration for other types of incidents

Where Affected?

- Identify the WHERE that will be affected in the scenario

Who Affected?

- Something that affects the company's ability to service customers but does not affect the customers directly

Scenario Based Planning

Incorporating multiple scenarios:

Group threat assessment scenarios by impact:

- Facilities
- Personnel
- Systems

Many scenarios will have multiple impacts

For example:

Fire = potential for Facility, Personnel, and System impact

Personnel Recovery

Have a well thought out and documented strategy for employees:

- Number of required personnel broken down by RTO
- Actual recovery locations
- Ensure proper infrastructure is in place
- Remote work capability?
  - Don’t put all of your eggs in this basket!
  - Power considerations – generators

Team Tasks

Does not matter how many teams are in the BCP, as long as all of the critical tasks are assigned, to include:

- Response and escalation
  - Assessment and declaration
- Technology Recovery
- Business Unit Recovery
- Restoration and return to normal operations

Communications

Creating thorough on-going plans:

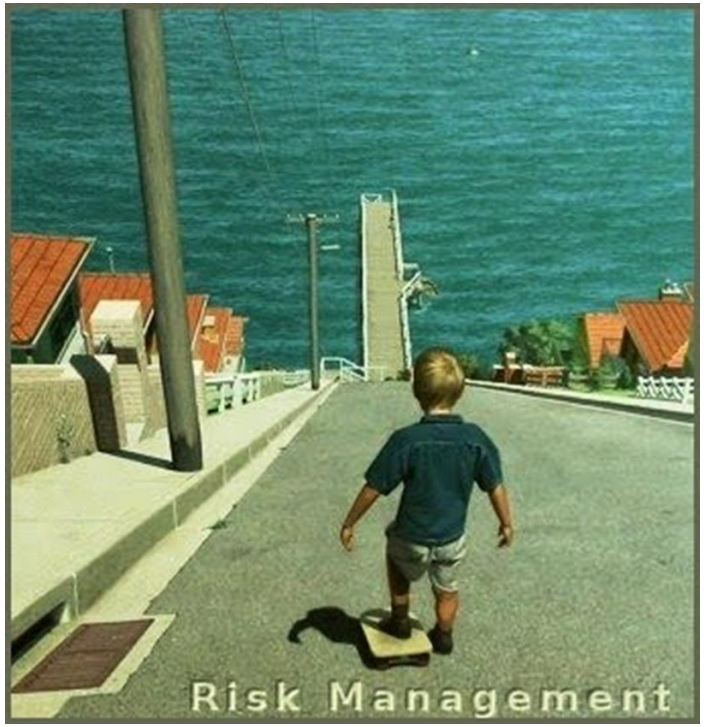
- Not just for onset of incident, but on-going
- Multiple communications vehicles
- Accessibility of contact lists
- Responsibility for initiating communications
- Frequency of contact information updates

Technology Recovery

- Are all critical systems accounted for? (Based off the BIA results)
- Are adequate resources available for successfully meeting RTOs?
  - Must include infrastructure requirements
  - Adequate hardware and software
  - Sufficient bandwidth
  - Personnel

Outsourcing – what can go wrong?

- Easily disappear
- Give you bad data
- Lose your information
- Cause data security exposure
- Under deliver
- **Be unprepared for a disaster**



Cybersecurity

- Including cyber events in the BCP and Risk Assessment
- Cross referencing the BCP and Incident Response Plan
- Incorporating cyber scenarios in testing

Testing

Schedule:

- More frequent, dynamic testing
- Test Plan: Should be multi-year (3 year)
- Should be multi year but no more than 3
- Rotate technologies of varying criticality
  - Low criticality do not necessarily need to be incorporated
- Must include supporting infrastructure
  - Build into RTOs
- Should be built off of most current BIA (Business Impact Analysis)

Types of Testing

Many ways to achieve “testing”

- **Evacuation Drills**
  - Floor wardens, meeting places
- **Communication Drills**
  - Call Trees
  - Automatic Notification Systems
- **Structured Walkthrough**
  - Smaller groups
  - Review specific details and tasks

Types of Testing

- **Simulation Testing**
  - Who is involved?
    - Experience
    - Authority
  - Incorporates Scenarios
    - Loss of building, technology, people
  - Decision making in a structured environment
  - Roles and Responsibilities
    - Technology
    - Business
  - Tests entire timeline of an event

Types of Testing

- **Technology Testing/ Functional Test/ Parallel Test**
  - Roles and Responsibilities
  - Validates RTOs and MADs for technologies that support business functions
  - Incorporate business lines for transaction processing

Ongoing Maintenance

- **BCP Updates should be at least yearly**
  - Employee/Team Members changes
  - Business function changes
  - Technology changes
  - Location changes
  - Third Party Provider changes

Thank You / Questions

Tracy Hall, MBCP
IT Assurance Manager
Wolf & Company, P.C
Direct: 413-726-6884
thall@wolfandco.com

Michael E. Kanarellis, HITRUST CCSFP
Principal
Director Healthcare IT Audit & Security Practice
Wolf & Company, P.C.
Direct (617) 428-5408
mkanarellis@wolfandco.com