

# RISK MANAGEMENT: PREPARING FOR A CRISIS

John Zuziak

5/12/2021

# Speaker

- IT Risk Management Practice Director for Change Healthcare
- 15 Years Cyber Security Experience
- Member of DHS / HHS Health Sector Coordinating Council
- Founding member of Greater Cincinnati health Information Roundtable
- Strategic Advisor to HealthGuard's eGRC
- Instructor for Harvard's CyberX Information Risk Management course



# What Are We Learning Here Today?

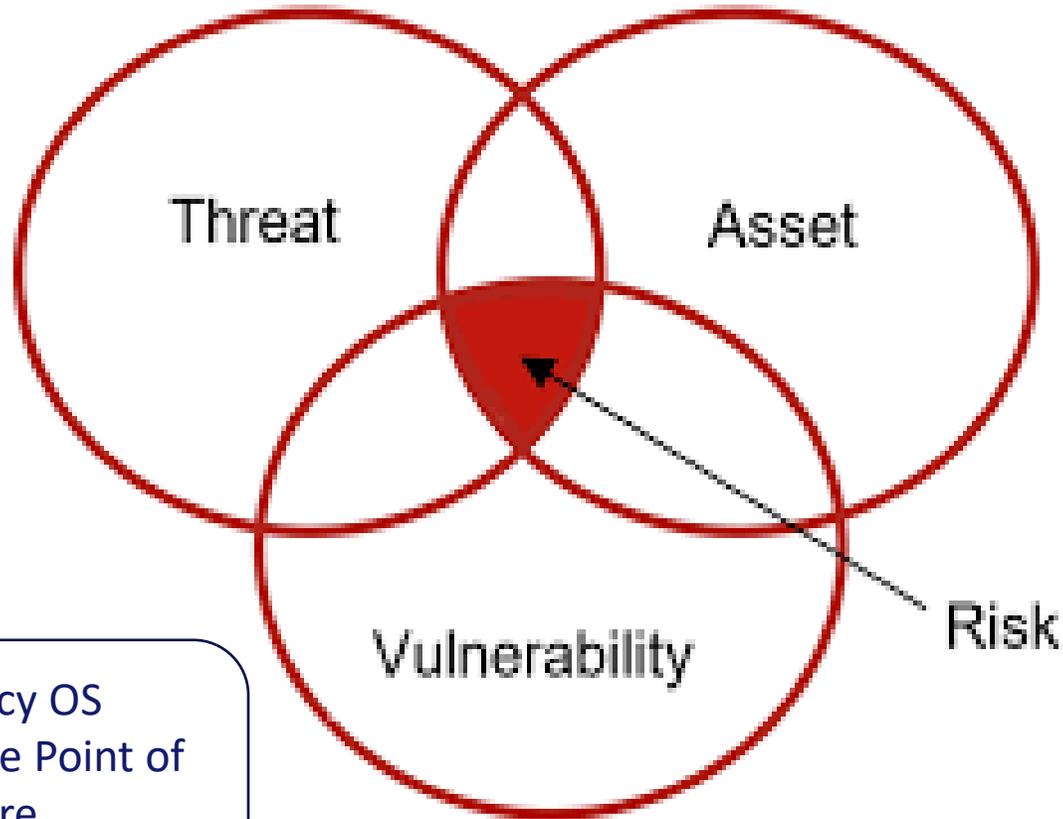
- How to measure and mitigate risk associated with data security
- Understand best practices related to cyber security and business continuity
- Integrate security and risk management into executive and staff training
- Develop and implement contingency plans



# Really? What is risk?

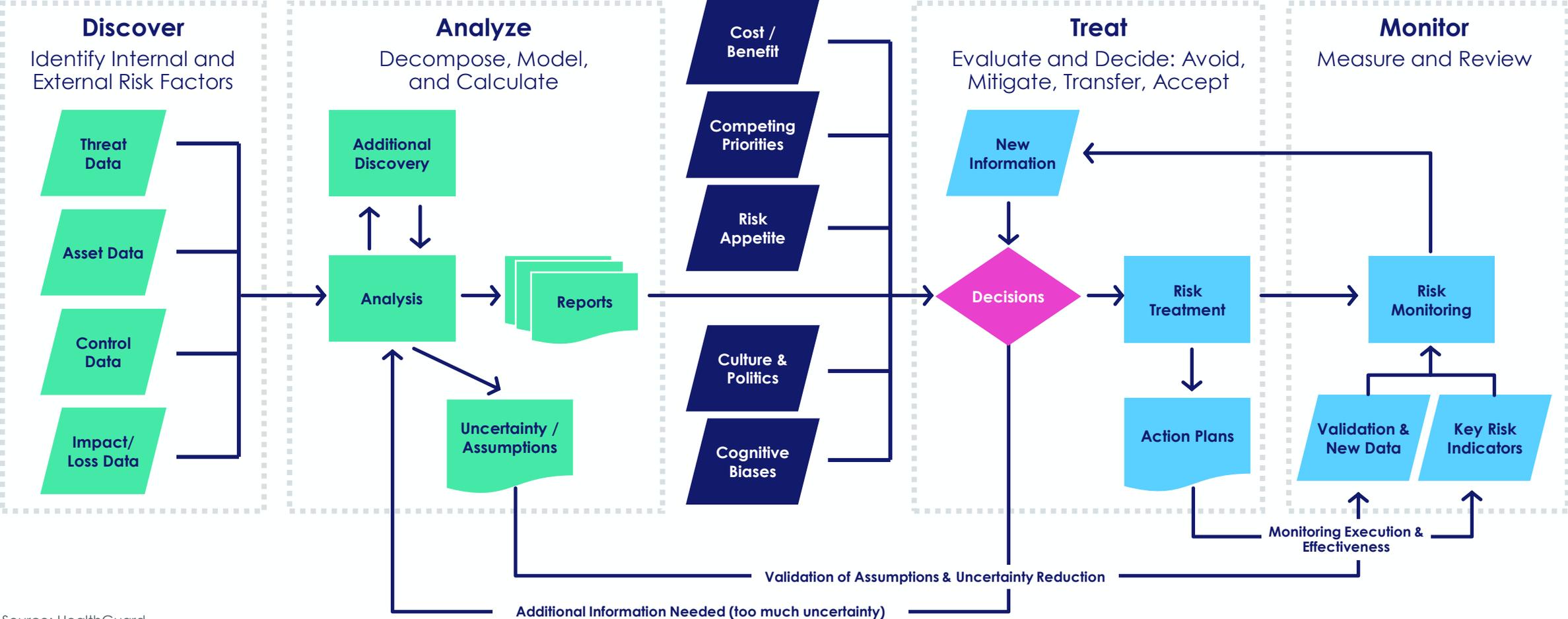
- Tornado
- Fire
- Pandemic
- Malware / Ransomware
- Phishing
- DDoS

- Legacy OS
- Single Point of Failure
- Untrained Staff



- Facility
- Data (Paper & Digital)
- IT Infrastructure
  - Laptop
  - Server
  - Database

# The Process



Source: HealthGuard

## Discover

## Analyze

## Treat

## Monitor

Disaster  
Recovery  
Requirements



Disaster Recovery  
Plan Development

Disaster Recovery  
Plan Exercise

What are the supporting resources upon which this process is critically dependent?



1. What would be the impact if this process were interrupted?
2. How quickly does it need to be restored?

Business Continuity  
Plan Development

Recovery  
Strategy

Recovery  
Capabilities

Teams

Procedures

Resources

Staff Relocation

Workload Transfer

Manual Workaround

Business Continuity  
Plan Exercise



Business  
Continuity  
Plan



# Requirements (Inventory)

Business Unit	Division		Department			
<input type="text"/>	<input type="text"/>		<input type="text"/>			
<span>RECOVERY PROCEDURES</span>	Department Description			<span>PLAN EXERCISE</span>		
	Process Name	Location	Process Manager		Process Description	RTO
			Primary	Backup		
<input type="button" value="BIA"/>						
<input type="button" value="STRATEGY"/>						
<input type="button" value="BIA"/>						
<input type="button" value="STRATEGY"/>						
<input type="button" value="BIA"/>						
<input type="button" value="STRATEGY"/>						
<input type="button" value="BIA"/>						
<input type="button" value="STRATEGY"/>						
<input type="button" value="BIA"/>						
<input type="button" value="STRATEGY"/>						

# The Details

### Impacts

Financial	Operational	Compliance & Legal	Reputation
Peak Impact [ ]	Peak Impact [ ]	Peak Impact [ ]	Peak Impact [ ]
Time Frame [ ]	Time Frame [ ]	Time Frame [ ]	Time Frame [ ]

### Recovery Time Objective

**Based upon the Peak Impacts & Time Frames, how quickly must this process be recovered?**

[ ]

**Briefly describe the primary justification for the selected Recovery Time Objective?**

[ ]

### Peak / Critical Time Periods

Time Of Day	Week Of Month
<input type="checkbox"/> NONE [ ]	<input type="checkbox"/> NONE [ ]
[ ]	[ ]
[ ]	[ ]
[ ]	[ ]

Day Of Week	Month Of Year
<input type="checkbox"/> NONE [ ]	<input type="checkbox"/> NONE [ ]
[ ]	[ ]
[ ]	[ ]
[ ]	[ ]
[ ]	[ ]

### Dependencies

Applications	Vendors / CHC Departments	Resources
<input type="checkbox"/> NONE [ ]	<input type="checkbox"/> NONE [ ]	<input type="checkbox"/> NONE [ ]
[ ]	[ ]	[ ]
[ ]	[ ]	[ ]
[ ]	[ ]	[ ]
[ ]	[ ]	[ ]
[ ]	[ ]	[ ]
[ ]	[ ]	[ ]
[ ]	[ ]	[ ]
[ ]	[ ]	[ ]

### CHC Products

Products Supported By This Process
<input type="checkbox"/> NONE [ ]
[ ]
[ ]
[ ]
[ ]
[ ]
[ ]
[ ]
[ ]

# Tabletops - What are our contingency plans?



# Strong BC/DR Plans Deliver Value!

## IT Service Continuity Mgmt

### Proactive measures reduce risk of disruption to IT services

- Support business continuity by **reducing the impact** of disruptive events
- Reduce IT vulnerabilities/risk to the business through **analysis and risk mgmt.**
- Prevent loss of valued reputation in addition to customer and user confidence
- Create tight **integration** between **ITSCM and BCM**

## Disaster Recovery & Testing

### Automate the compliance process...eliminate complexity

- Define and understand **DR architecture options** (SRM, HA, etc.)
- Implement technology to **simplify DR Testing** and Recovery
- Define **DR architecture standards** ... enforce through Enterprise Architecture

## Critical Business Process Alignment

### Understand business impact of disruption to IT services

- Establish **applications mappings** to servers and datacenters
- Map applications to **critical business processes**
- Institutionalize **mechanisms** to establish and maintain governance

## Meet Compliance Requirements

### Win at compliance 100% of the time

- Define, align with, and meet enterprise, Managed Solutions, and Corporate **Enterprise Risk Management** compliance requirements for Disaster Recovery and Business Continuity

# Questions?

# Further Questions?



**Email** John Zuziak

[john.zuziak@ChangeHealthcare.com](mailto:john.zuziak@ChangeHealthcare.com)

# CHANGE HEALTHCARE