DRJ SPRING 2020
March 15-18, Orlando

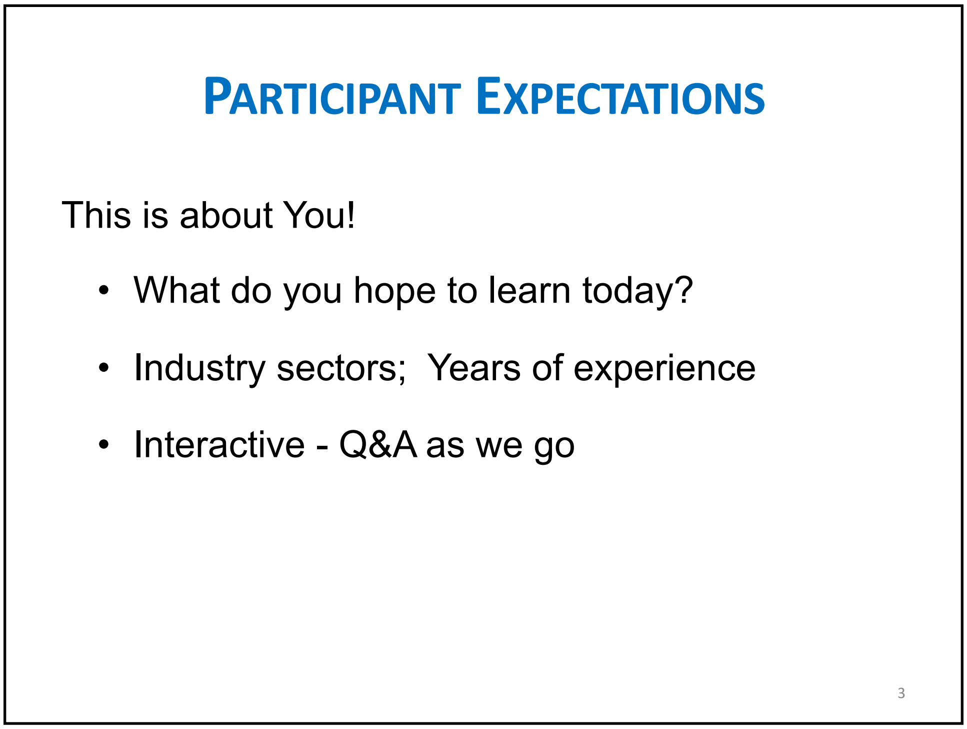
Risk: How to Identify Critical Risk within Your Organization

Joe Layman, MIS, CBCP, ITIL, CRISC
Head of Enterprise Business Continuity Management

Susan Zielan, CBCP
Senior BCM Program Manager

SESSION AGENDA

- *Identify* critical risks that matter
- Criteria to *prioritize*: most to least critical
- *Define* the risk as an asset, vulnerability or threat
- Approaches to *mitigate* critical risks



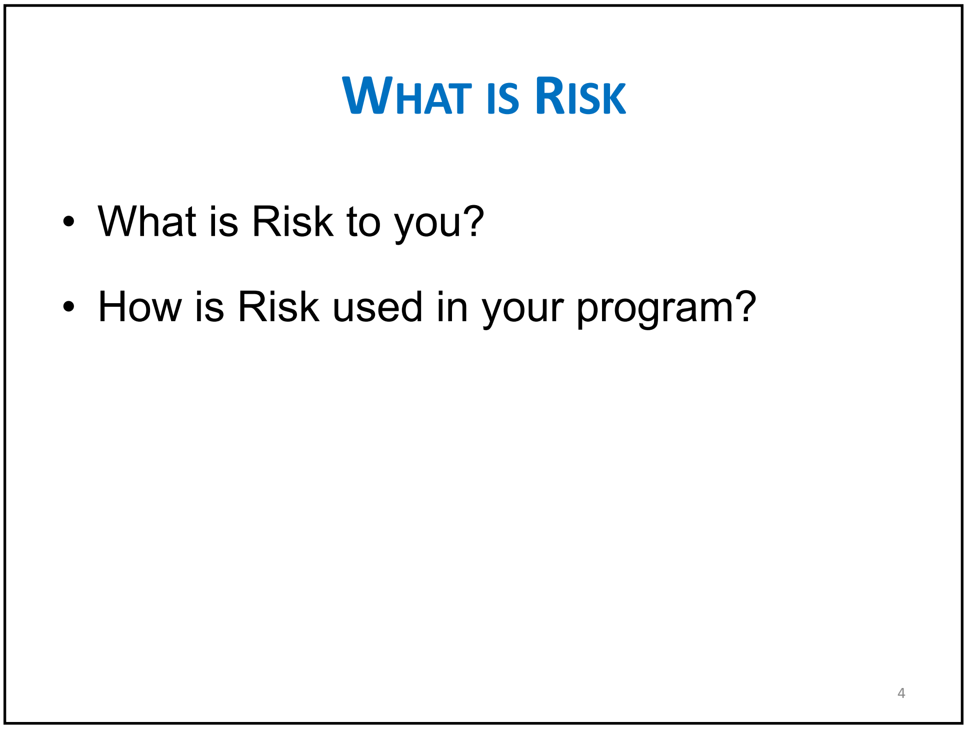
PARTICIPANT EXPECTATIONS

This is about You!

- What do you hope to learn today?
- Industry sectors; Years of experience
- Interactive - Q&A as we go

3

3



WHAT IS RISK

- What is Risk to you?
- How is Risk used in your program?

4

4

WHAT IS RISK

How do your Program risks (BC, DR, EM/IM/CM) align with C-Suite risks and Mission Statement?

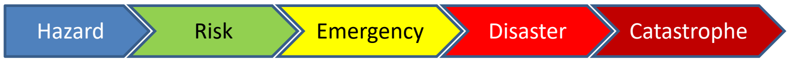
DRJ Glossary

- Potential for exposure to loss
  which can be determined by using either
  qualitative (#) or quantitative ($) measures.

- Combination of the probability of an incident and its consequence

EVOLUTION OF RISK

Term	Definition
Hazard	A source of danger that may or may not lead to an emergency or disaster. -- National Governors Association 1982
Risk	A risk is represented by the likelihood of the hazard leading to an actual disruption and the resulting impact should it occur
Emergency	A product of a realized hazard, typically characterized as a situation exhibiting negative consequences that requires the efforts of one or more emergency services – Fire, Police, EMS, Public Health or other – to manage
Disaster	The response to an emergency exceeds the capabilities of established emergency services in one or more critical areas such as shelter, fire suppression or mass care for a particulate local government or region.
Catastrophe	The response requirements in one or more areas are unable to be met at all levels of government. Usually requires a response at the national level



Risk Assessment

The overall process of

- Risk Identification
- Risk Analysis
- Risk Evaluation

DRJ 2018

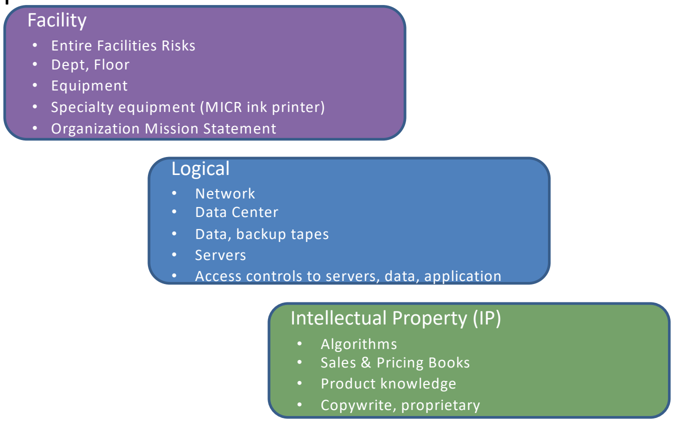
HAZARD
VS
RISK
A HAZARD is something that has the potential to harm you
RISK is the likelihood of a hazard causing harm

A systematic approach to identifying hazard or risks
that are most likely to have an impact
on a facility and the surrounding community.

HHS.gov 2017 (HVA)

Asset

Types of Risk



Facility

- Entire Facilities Risks
- Dept, Floor
- Equipment
- Specialty equipment (MICR ink printer)
- Organization Mission Statement

Logical

- Network
- Data Center
- Data, backup tapes
- Servers
- Access controls to servers, data, application

Intellectual Property (IP)

- Algorithms
- Sales & Pricing Books
- Product knowledge
- Copywrite, proprietary

VULNERABILITY

Inherent vulnerabilities just by doing business

Vendor

- Target Breach – HVAC backdoor vulnerability
- Partners – Gov't esp.
- Network Access
- VPN, Citrix
- Pen Tests

Outsourced Vendor

- Data Center, Call Center
- Security, IT
- Developers
- Payroll, Xerox, Janitorial
- Amenities – coffee, vending, catering

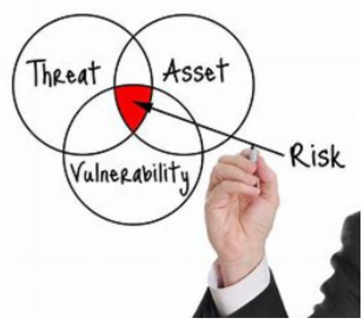
Other

- Credential sharing, Tailgating
- Clients
- USB, External drives
- Cyber attack; other external actors
- Technology – apps, software, OS, patches, virus, equipment
- Outlook Web Access; BYOD – MDM (Mobile Device Manager)

THREAT

Eliminating risks involves reducing threats and vulnerabilities

- Threats originate outside a system
- Vulnerabilities are an inherent weakness of a system
- Vulnerability is used to create a real threat to a system



THREAT – EXTERNAL

Security Risks

- Policy
- Privacy
- Passwords
- Computer Theft
- Blackmail
- Social Engineering
- Terrorism
- Virus

Physical Risks

- Badge Access
- Tenants, Neighbors
- Airport, Docks, Trains
- Employees, Visitors, Vendors
- Active Shooter
- Kidnap & Ransom

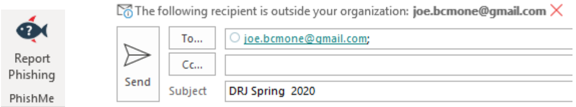
Cyber Risks

- Malware / Adware
- Keylogger
- Virus
- Firewalls
- Social Engineering
- Phishing
- Ransomware
- Mobile & the Cloud

11

THREAT – EXTERNAL

Phishing Risk



The following recipient is outside your organization: **joe.bcmone@gmail.com**

To... joe.bcmone@gmail.com;

Subject DRJ Spring 2020

[External Content] This message is from an external source. Please exercise caution when opening attachments or links.

EXTERNAL EMAIL: Please do not click any links or open any attachments unless you trust the sender and know the content is safe.

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Mitigation

- Desktop/PC
  - → Click on the Email icon
  - → Forward to Phishing@company.com
- Mobile device
  - → You clicked on it, now it's on your device, within your corporate email.
  - → Forward to yourself, now it's in your personal email, tablet, or pc.

12

COMPLACENCY

Complacency

- That's the way it's always been
  - Formal or informal acceptance
- This will never happen to me/us - Denial
- That belongs to someone else, not me!
  - Lack of ownership, avoidance
- It was reported
  - Assuming it has been addressed

Mitigation

- Each risk should have supporting documentation
- Think of an audit process – what is needed to mitigate the issue
- Controls (Mitigate what you can)
- Training and awareness

Complacency

That's the way it's always been - formal or informal acceptance

This will never happen to me/us - denial

That belongs to someone else, not me! – ownership, avoidance

It was reported - assuming it has been addressed

Mitigation

Each risk should have supporting documentation

Think of an audit process – what is needed to mitigate the issue

Controls (Mitigate what you can)

BUSINESS CONTINUITY INCIDENT CATEGORIES

Risk Avoidance

- An informed decision not to become involved in or to withdraw from a risk situation
- Remove or replace the risk or the impact from risk
- Stay out of the water

Risk Tolerance

→ Initially Defer

- A measure of the degree of uncertainty an entity is willing to accept in respect of negative changes to business or assets
- The degree of variability in returns that an entity is willing to stand

Risk Mitigation

- Implementation of measures to deter specific threats to the business operations and/or respond to any occurrence of such threats in a timely and appropriate manner.
- Activities taken to eliminate/reduce the severity or consequences of an emergency.

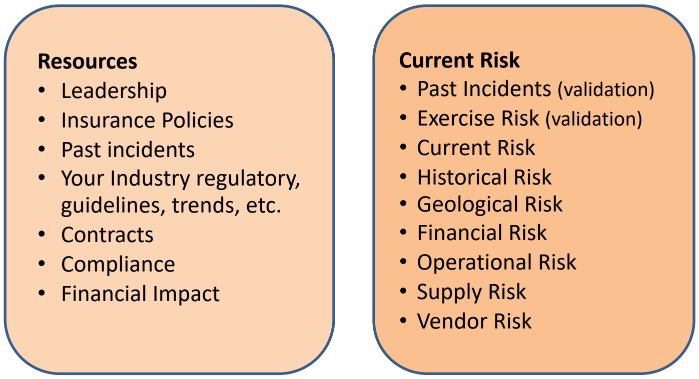
Risk Acceptance

- A management decision to take no action to mitigate the impact of a particular risk.

Identify Risk

Identify Risk – What keeps your C-Suite up at night?

Where to find the risks that impact me:



Resources
- Leadership
- Insurance Policies
- Past incidents
- Your Industry regulatory, guidelines, trends, etc.
- Contracts
- Compliance
- Financial Impact

Current Risk
- Past Incidents (validation)
- Exercise Risk (validation)
- Current Risk
- Historical Risk
- Geological Risk
- Financial Risk
- Operational Risk
- Supply Risk
- Vendor Risk

Build Your Assessment

Foundation and alignment

- Your Risks
- C-Suite Risks
- Other Resources
- Organization Mission Statement

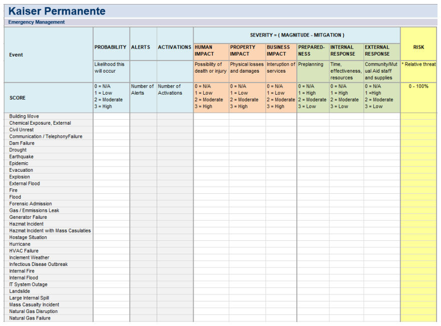
HVA OR RISK TEMPLATE

Using the Template (Handout)

- Risks
  - Down the left side
  - Add, Delete, Combine according to your company risks
- Impacts
  - Across the top
- Scoring & Weighting and Scoring Methods
  - Identify criticality with weighting
  - Include the Legend across the top
  - Scale 1, 2, 3, etc.   Make it easy

RISK TEMPLATES

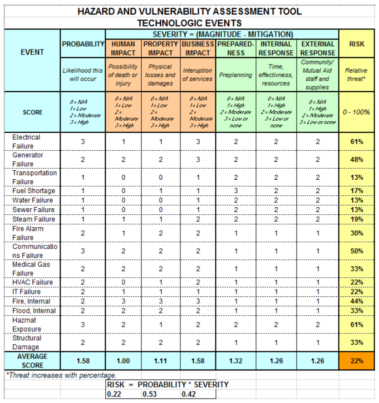
Templates – use any current templates



Kaiser Permanente

Emergency Management

Event	PROBABILITY	ALERTS	ACTIVATIONS	SEVERITY = (MAGNITUDE - MITGATION)						RISK
				HUMAN IMPACT	PROPERTY IMPACT	BUSINESS IMPACT	PREPARED-NESS	INTERNAL RESPONSE	EXTERNAL RESPONSE	
	Likelihood this will occur			Possibility of dealth or injury	Physical losses and damages	Interuption of services	Preplanning	Time, effectiveness, resources	Community/Mutual Aid staff and supplies	* Relative threat
SCORE	0 = N/A 1 = Low 2 = Moderate 3 = High	Number of Alerts	Number of Activations	0 = N/A 1 = Low 2 = Moderate 3 = High	0 = N/A 1 = Low 2 = Moderate 3 = High	0 = N/A 1 = Low 2 = Moderate 3 = High	0 = N/A 1 = High 2 = Moderate 3 = Low	0 = N/A 1 = High 2 = Moderate 3 = Low	0 = N/A 1 =High 2 = Moderate 3 = Low	0 - 100%
Building Move										
Chemical Exposure, External										
Civil Unrest										
Communication / TelephonyFailure										
Dam Failure										
Drought										
Earthquake										
Epidemic										
Evacuation										
Explosion										
External Flood										
Fire										
Flood										
Forensic Admission										
Gas / Emmissions Leak										
Generator Failure										
Hazmat Incident										
Hazmat Incident with Mass Casulaties										
Hostage Situation										
Hurricane										
HVAC Failure										
Inclement Weather										
Infectious Diseae Outbreak										
Internal Fire										
Internal Flood										
IT System Outage										
Landslide										
Large Internal Spill										
Mass Casualty Incident										
Natural Gas Disruption										
Natural Gas Failure										



HAZARD AND VULNERABILITY ASSESSMENT TOOL

TECHNOLOGIC EVENTS

EVENT	PROBABILITY	SEVERITY = (MAGNITUDE - MITIGATION)						RISK
		HUMAN IMPACT	PROPERTY IMPACT	BUSINESS IMPACT	PREPARED-NESS	INTERNAL RESPONSE	EXTERNAL RESPONSE	
	Likelihood this will occur	*Possibility of death or injury*	*Physical losses and damages*	*Interuption of services*	*Preplanning*	*Time, effectivness, resources*	*Community/ Mutual Aid staff and supplies*	*Relative threat**
SCORE	*0 = N/A 1 = Low 2 = Moderate 3 = High*	*0 = N/A 1 = Low 2 = Moderate 3 = High*	*0 = N/A 1 = Low 2 = Moderate 3 = High*	*0 = N/A 1 = Low 2 = Moderate 3 = High*	*0 = N/A 1 = High 2 = Moderate 3 = Low or none*	*0 = N/A 1 = High 2 = Moderate 3 = Low or none*	*0 = N/A 1 = High 2 = Moderate 3 = Low or none*	*0 - 100%*
Electrical Failure	3	1	1	3	2	2	2	61%
Generator Failure	2	2	2	3	2	2	2	48%
Transportation Failure	1	0	0	1	2	2	2	13%
Fuel Shortage	1	0	1	1	3	2	2	17%
Water Failure	1	0	0	1	2	2	2	13%
Sewer Failure	1	0	0	1	2	2	2	13%
Steam Failure	1	1	1	2	2	2	2	19%
Fire Alarm Failure	2	1	2	2	1	1	1	30%
Communications Failure	3	2	2	2	1	1	1	50%
Medical Gas Failure	2	2	2	2	1	1	1	33%
HVAC Failure	2	0	1	2	1	1	1	22%
IT Failure	2	1	1	1	1	1	1	22%
Fire, Internal	2	3	3	3	1	1	1	44%
Flood, Internal	2	2	2	2	1	1	1	33%
Hazmat Exposure	3	2	1	2	2	2	2	61%
Structural Damage	2	2	2	2	1	1	1	33%
AVERAGE SCORE	1.58	1.00	1.11	1.58	1.32	1.26	1.26	22%

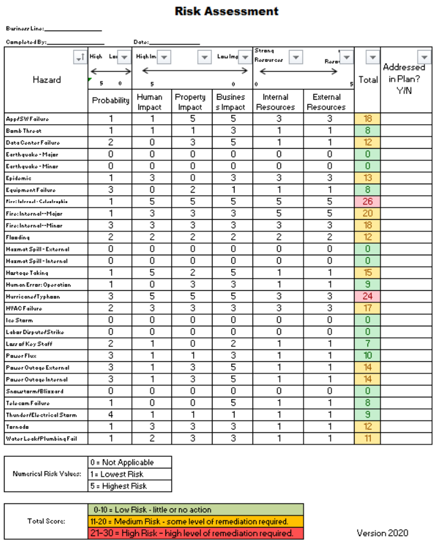
**Threat increases with percentage.*

RISK = PROBABILITY * SEVERITY		
0.22	0.53	0.42

Download here
https://www.calhospitalprepare.org/hazard-vulnerability-analysis

FEMA Risk Template

FEMA Template



Risk Assessment

Business Line:________________

Completed By:________________ Date:______________

Hazard	High Lo 5 0	High Im 5		Low Imp 0	Strong Resources 0	Reso 5	Total	Addressed in Plan? Y/N
	Probability	Human Impact	Property Impact	Busines s Impact	Internal Resources	External Resources		
App/SW Failure	1	1	5	5	3	3	18	
Bomb Threat	1	1	1	3	1	1	8	
Data Center Failure	2	0	3	5	1	1	12	
Earthquake - Major	0	0	0	0	0	0	0	
Earthquake - Minor	0	0	0	0	0	0	0	
Epidemic	1	3	0	3	3	3	13	
Equipment Failure	3	0	2	1	1	1	8	
Fire: Internal - Catastrophic	1	5	5	5	5	5	26	
Fire: Internal--Major	1	3	3	3	5	5	20	
Fire: Internal--Minor	3	3	3	3	3	3	18	
Flooding	2	2	2	2	2	2	12	
Hazmat Spill - External	0	0	0	0	0	0	0	
Hazmat Spill - Internal	0	0	0	0	0	0	0	
Hostage Taking	1	5	2	5	1	1	15	
Human Error: Operation	1	0	3	3	1	1	9	
Hurricane/Typhoon	3	5	5	5	3	3	24	
HVAC Failure	2	3	3	3	3	3	17	
Ice Storm	0	0	0	0	0	0	0	
Labor Dispute/Strike	0	0	0	0	0	0	0	
Loss of Key Staff	2	1	0	2	1	1	7	
Power Flux	3	1	1	3	1	1	10	
Power Outage External	3	1	3	5	1	1	14	
Power Outage Internal	3	1	3	5	1	1	14	
Snowstorm/Blizzard	0	0	0	0	0	0	0	
Telecom Failure	1	0	0	5	1	1	8	
Thunder/Electrical Storm	4	1	1	1	1	1	9	
Tornado	1	3	3	3	1	1	12	
Water Leak/Plumbing Fail	1	2	3	3	1	1	11	

Numerical Risk Values:	0 = Not Applicable
	1= Lowest Risk
	5 = Highest Risk

Total Score:	0-10 = Low Risk - little or no action
	11-20 = Medium Risk - some level of remediation required.
	21-30 = High Risk – high level of remediation required.

Version 2020

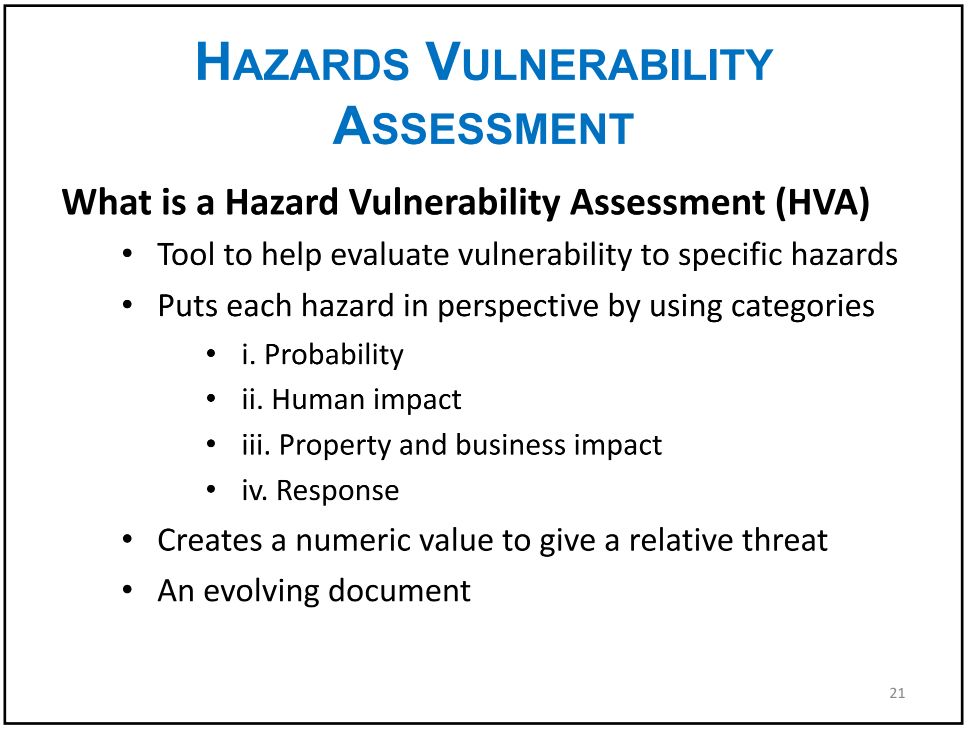
https://www.fema.gov/

Risk Assessment

Risk Assessment / Analysis

- *Identify* the risks to an organization
- *Assess* the critical functions necessary for an organization to continue business operations
- *Define* the controls in place to reduce organization exposure
- *Evaluate* the cost for such controls

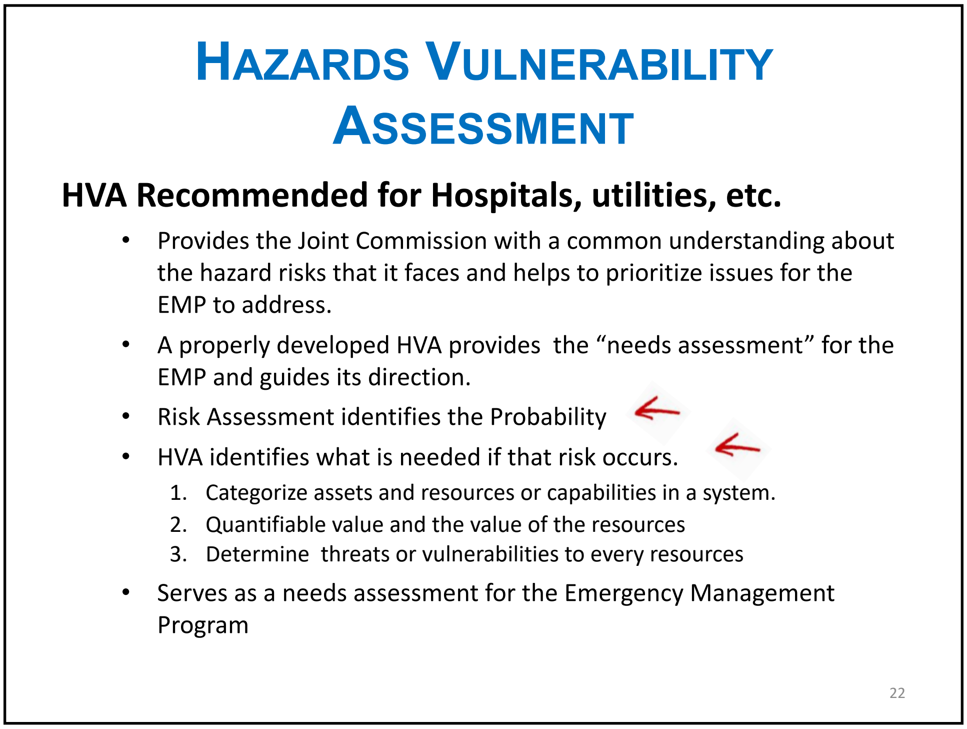
DRJ 2020



Hazards Vulnerability Assessment

What is a Hazard Vulnerability Assessment (HVA)

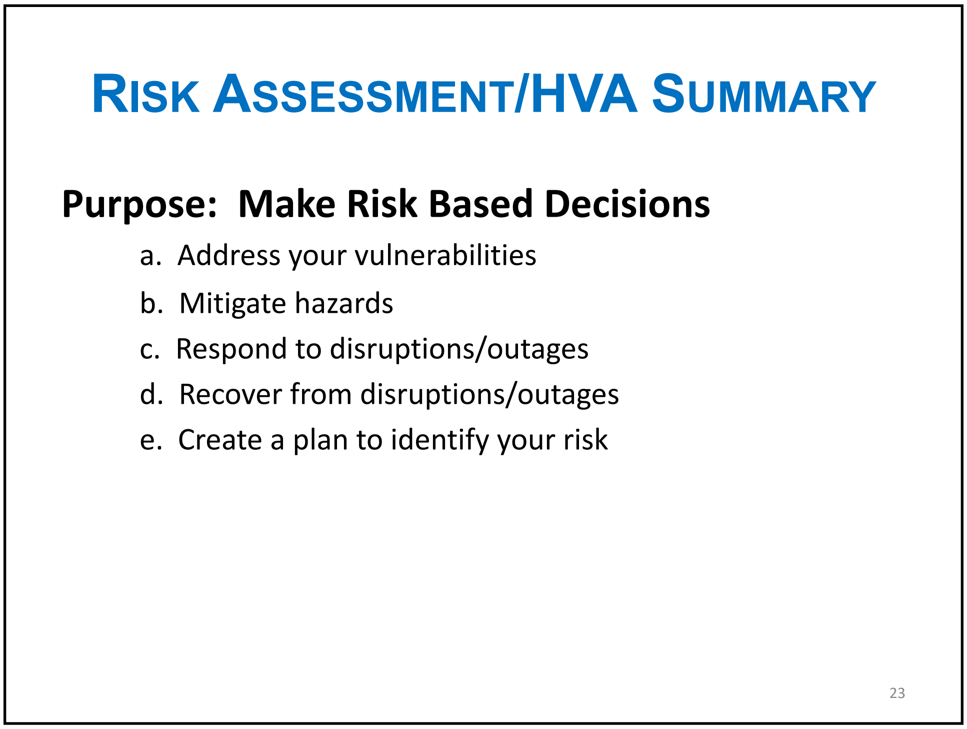
- Tool to help evaluate vulnerability to specific hazards
- Puts each hazard in perspective by using categories
  - i. Probability
  - ii. Human impact
  - iii. Property and business impact
  - iv. Response
- Creates a numeric value to give a relative threat
- An evolving document



Hazards Vulnerability Assessment

HVA Recommended for Hospitals, utilities, etc.

- Provides the Joint Commission with a common understanding about the hazard risks that it faces and helps to prioritize issues for the EMP to address.
- A properly developed HVA provides the "needs assessment" for the EMP and guides its direction.
- Risk Assessment identifies the Probability ←
- HVA identifies what is needed if that risk occurs. ←
  1. Categorize assets and resources or capabilities in a system.
  2. Quantifiable value and the value of the resources
  3. Determine threats or vulnerabilities to every resources
- Serves as a needs assessment for the Emergency Management Program



RISK ASSESSMENT/HVA SUMMARY

Purpose: Make Risk Based Decisions

a. Address your vulnerabilities

b. Mitigate hazards

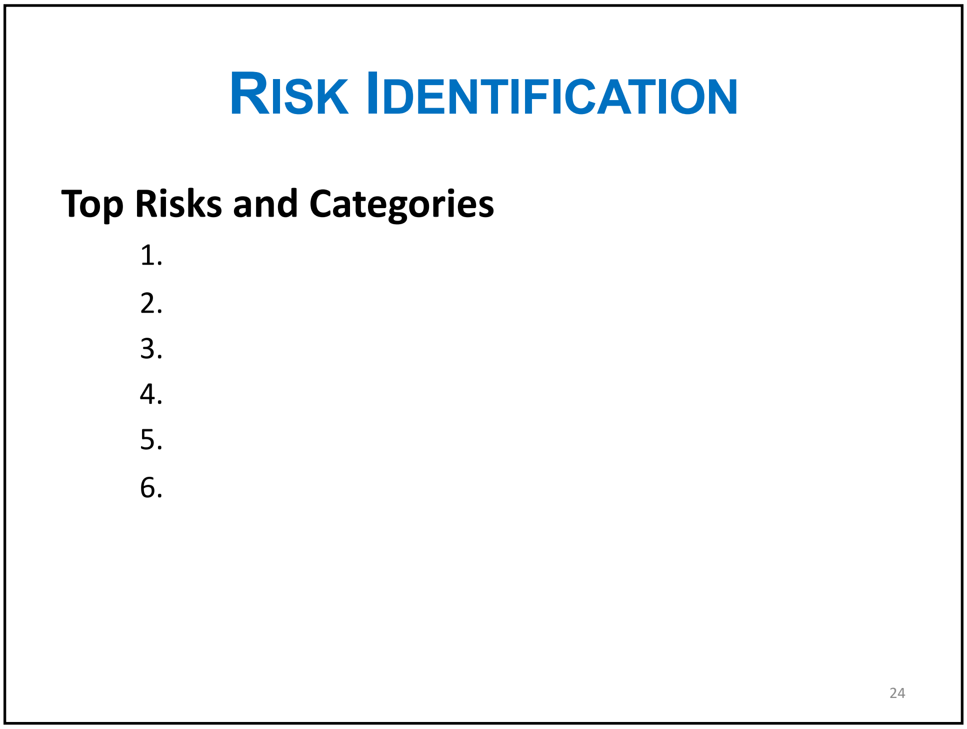
c. Respond to disruptions/outages

d. Recover from disruptions/outages

e. Create a plan to identify your risk

23

23



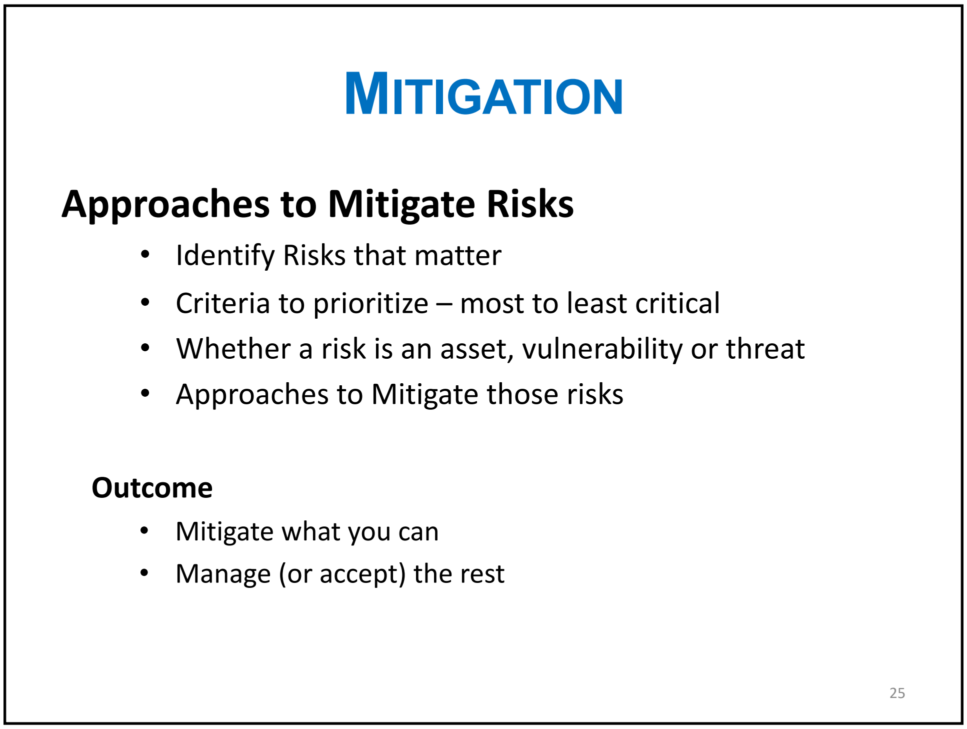
RISK IDENTIFICATION

Top Risks and Categories

1.
2.
3.
4.
5.
6.

24

24



MITIGATION

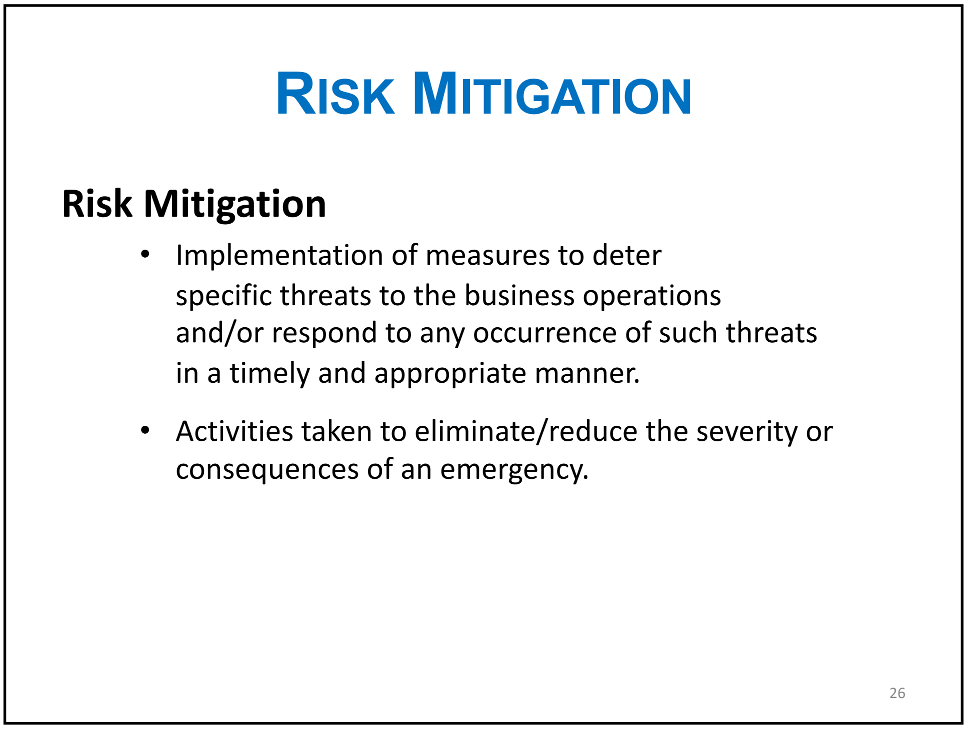
Approaches to Mitigate Risks

- Identify Risks that matter
- Criteria to prioritize – most to least critical
- Whether a risk is an asset, vulnerability or threat
- Approaches to Mitigate those risks

Outcome

- Mitigate what you can
- Manage (or accept) the rest

25



RISK MITIGATION

Risk Mitigation

- Implementation of measures to deter specific threats to the business operations and/or respond to any occurrence of such threats in a timely and appropriate manner.
- Activities taken to eliminate/reduce the severity or consequences of an emergency.

26

Case Study

Kaiser Permanente, January 17 – 27, 2020

Kaiser Woodland Hills canceling surgeries after main break leaves hospital without water service

Los Angeles Department of Water and Power spokeswoman Christina Holland said the utility's crews did not respond because the water line break occurred somewhere in the hospital's own water system, not in pipes controlled by the utility.

All patients removed from Kaiser Woodland Hills amid temporarily closure after water main break

Kaiser Permanente Woodland Hills Medical Center resumed full operations today after securing all required county and state approvals following the repair of a water main break.

Hospital services — including the Emergency Department, Urgent Care, and pharmacy — are fully operational. All scheduled appointments will resume on Monday, Jan. 27.

Kaiser Permanente Woodland Hills Won't Have Running Water Until Thursday (At The Earliest)

BY KYLE STOKES IN NEWS ON JANUARY 20, 2020 2:45 PM

"We sincerely apologize for any inconvenience the campus temporary closure may cause to our members, patients, physicians, staff and community,"

The medical center said it is unclear when water will be restored.

Monday, January 20, 2020 3:47PM

WOODLAND HILLS, LOS ANGELES (KABC) -- Surgeries and appointments were canceled at Kaiser Permanente Medical Center in Woodland Hills after a main break has left the hospital without water service for more than 36 hours.

The break happened Saturday night. Hospital officials say they are not evacuating current patients and not closing the emergency room.

27

Internal Collaboration

Coordinate and Validate Risk Among Teams

- BC Risk Assessment
- EM HVA
- DR Risk Assessment
- IT/InfoSec
  - IT
  - Vendor Risk
  - Physical Risk

28

Vendor Management

Does your Vendor pose a Risk?

- Critical Vendors – have you reviewed/signed off on their plans?
- Does this create cascading business risks for your organization?
- Onshore vs Offshore Vendor – specifically political risk?
- Staff Relocation – Continuity or Alternate Housing?
- Fire, Facilities, Office
  - Sub-lease – what the Landlord covers including timeframes
  - Tenants have insurance covering business and belongings – cubes, walls, desk, PCs, printers,
- How quickly get your building up an running? RentSys, SunGard, Agility
- Exclusions – pay more out of pocket; first $100k is your responsibility
- Cyber

Operational Risk

- How soon will operations be up and running; in what % capacity?
- Financial reserves to meet the deductible and anything else that may come up

Additional Sources

Tribal knowledge

- Type of incidents
- Frequency
- Neighbor company risk, hazmat, etc., other risks
- Neighbor risk assessment

Contracts

- Line of Business, Contract, SLAs, Requirements
- Force Majeure – duration vs. restoration time

Policies

- Business Interruption
- Cyber
- Error and Omissions – Protects the board members

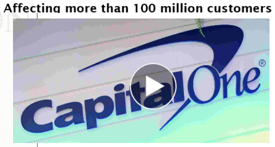
REPUTATION

Don’t let this happen to you

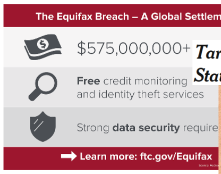
Thousands of Disney Plus accounts were hacked and sold online for as little as $3

FACEBOOK HIT BY FINES
$5 billion
by the FTC for privacy violations
announced a few days ago that
THE DEBRIEF | FACEBOOK'S PRIVACY FINE
FTC fines social media company $5 billion over handling of user data

Massive data breach hits Capital One, Affecting more than 100 million customers



Anthem Hit by Massive Data Breach



The Equifax Breach – A Global Settlement

$575,000,000+

Free credit monitoring and identity theft services

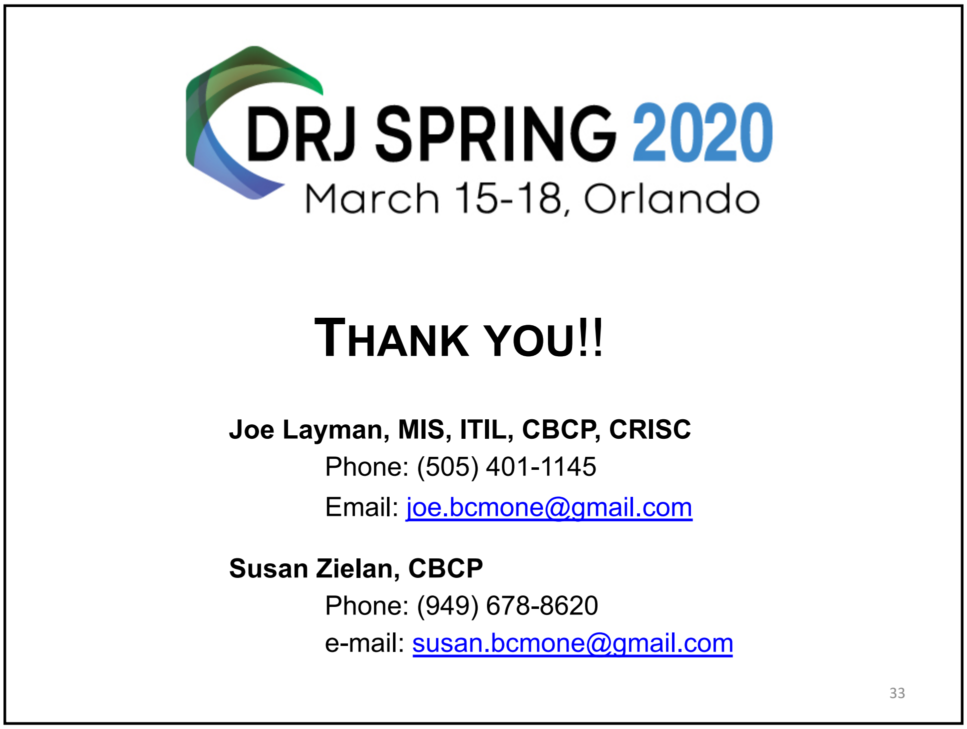
Strong **data security** require

➡ Learn more: ftc.gov/Equifax

Target to Pay $18.5 Million to 47 States in Security Breach Settlement

Security Breach leaves approximately 56 million credit and debit card numbers exposed.

QUESTIONS



DRJ SPRING 2020
March 15-18, Orlando

THANK YOU!!

Joe Layman, MIS, ITIL, CBCP, CRISC
Phone: (505) 401-1145
Email: joe.bcmone@gmail.com

Susan Zielan, CBCP
Phone: (949) 678-8620
e-mail: susan.bcmone@gmail.com

33

33