INTEGRATING CYBER SECURITY PREPAREDNESS INTO AN EMERGENCY MANAGEMENT PROGRAM

ROBERT BALLESTEROS

#IAEM17

OVERVIEW

- Why we care about cyber security
- Emergency Management vs. Cyber Security Preparedness, a comparison
- How I see Emergency Management (Preparedness)
- Integrating cyber security into your program
- Questions and wrap up

WHY DO WE CARE ABOUT CYBERSECURITY?

Cyber threat actors regularly target government and industry to:

- Steal intellectual property
- Commit financial fraud
- Damage the corporate brand
- Cause a business incident

"Yahoo says 1 billion user accounts were hacked"

The New York Times – December 14, 2016

"Hackers trigger yet another power outage in Ukraine"

Ars Technica – January 11, 2017

"Cyberattack on German steel plant caused significant damage"

Security Week – December 18, 2014

> Cyber espionage is "the greatest transfer of wealth in history"
>
> *- Former National Security Agency Director, General Keith B. Alexander July 9, 2012*

CYBER THREAT ACTORS

Nation States

- Highly Skilled
- Objectives
  - Espionage
  - Competitive Advantage
- Targeting Method
  - Watering holes, spear phishing
- Long-term Operations
  - Strategic actions

Hacktivists & Thrill Seekers

- Minimally Skilled
- Objectives
  - Brand Damage
  - Publicity
  - Thrill and notoriety
- Targeting Methods
  - Simple publicly-available tools
- Short-term Operations

Cyber Criminals

- Moderately to Highly Skilled
- Objectives
  - Financial gain
  - Notoriety
- Targeting Method
  - Phishing messages
  - Drive-by downloads
- Long-term Operations

Non-State Actors

- Moderately Skilled
- Objectives
  - Espionage
  - Financial gain
- Targeting Methods
  - Phishing, spear phishing, watering holes
  - Publicly-available tools
- Short-term Operations

TARGETING METHODS

Spearphishing

- Highly targeted
  - Difficult to identify
- Specific to the target
  - Designed to deceive
- Data often gathered through online research
  - Social media; publicly available data
- Contains malicious links and / or attachments
  - May infect computer systems
  - Leads to fraudulent login pages

Web Exploits

- Exploits browser
  - Security flaws
- No need to click or download
  - Only need to visit site
- Often legitimate websites
  - Compromised with malicious code
- Watering Holes
  - More specific type of drive-by download
  - Infect sites of common interest to targets

Removable Media Devices

- USB drives
  - Thumb drives
  - Flash drives
  - Smartphones
  - MP3 players
- Infect machines when plugged in
  - Contains viruses / malware
- Can be easily misplaced or stolen
  - Contain sensitive company information

Webmail / Social Media

- Social engineering
  - Human interaction
  - “Con artists”
- Pose as colleague or executive requesting action
  - Email links and attachments
  - Wire transfers
  - IT professional
- Social media research
  - Facebook and LinkedIn

CYBER EVENT VS CYBER INCIDENT

What's the difference between….

Cyber event

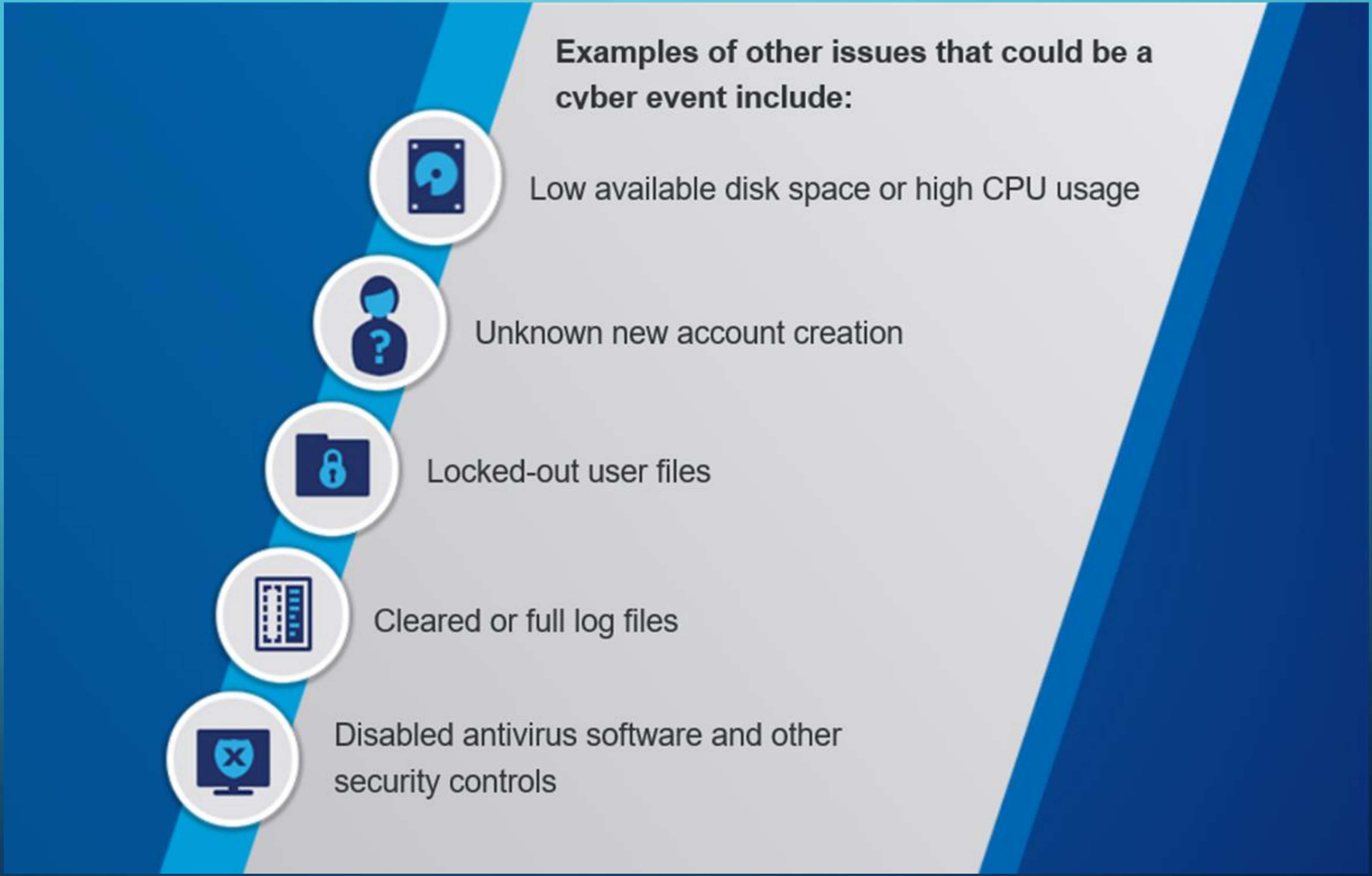
VS

Cyber incident

An event referring to any observable occurrence in a system or network that is suspected as malicious.

An incident that threatens the security, confidentiality, integrity, or availability of critical assets.

CYBER EVENT EXAMPLES



Examples of other issues that could be a cyber event include:

Low available disk space or high CPU usage

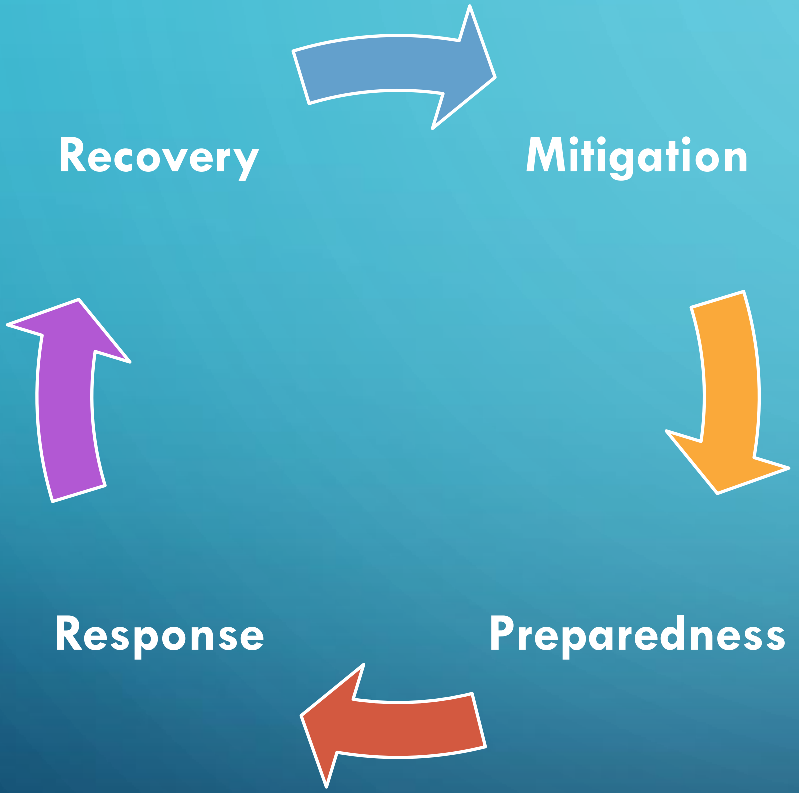
Unknown new account creation

Locked-out user files

Cleared or full log files

Disabled antivirus software and other security controls

PHASE OF EMERGENCY MANAGEMENT



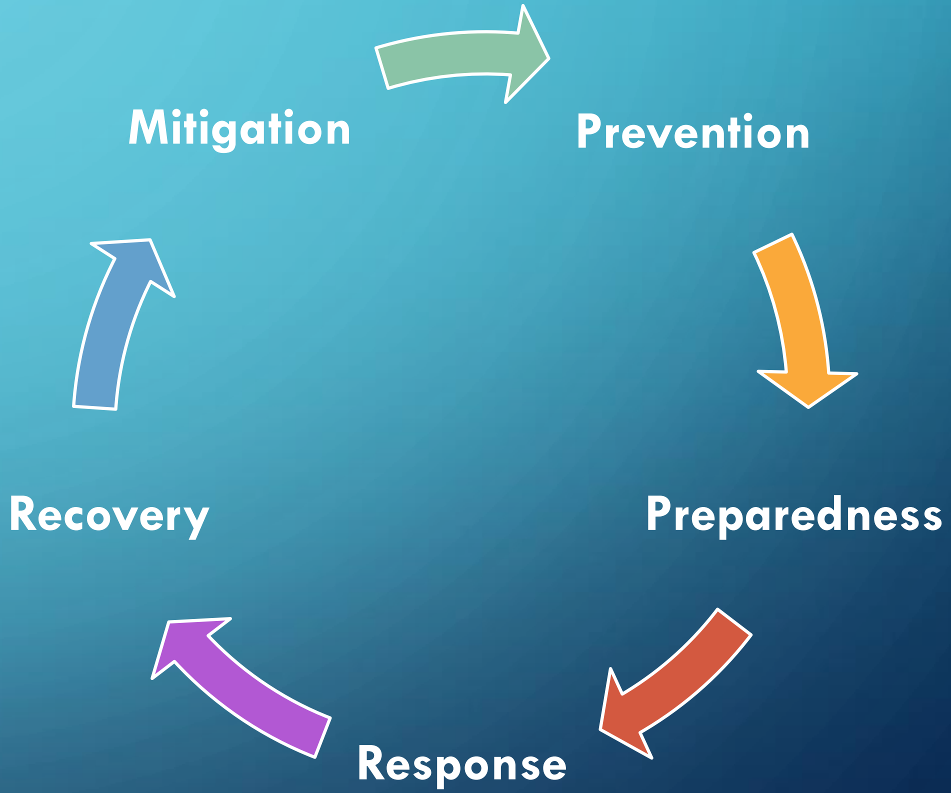
Recovery

Mitigation

Preparedness

Response

OR



Mitigation

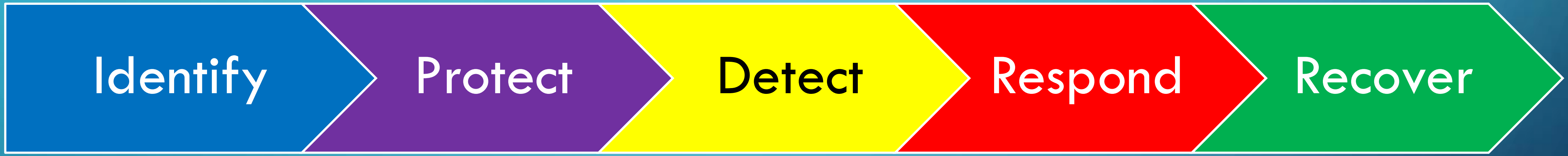
Prevention

Preparedness

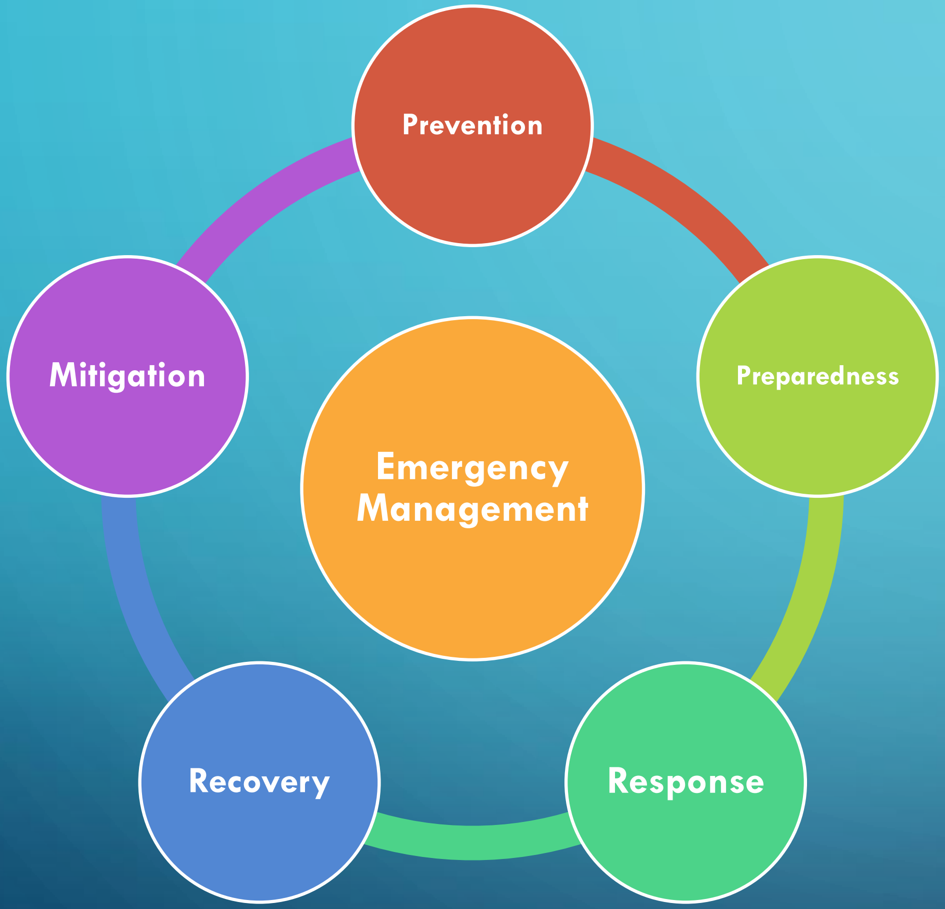
Response

Recovery

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) CYBERSECURITY FRAMEWORK



EMERGENCY MANAGEMENT VS. CYBER SECURITY PREPAREDNESS - A COMPARISON



Emergency Management

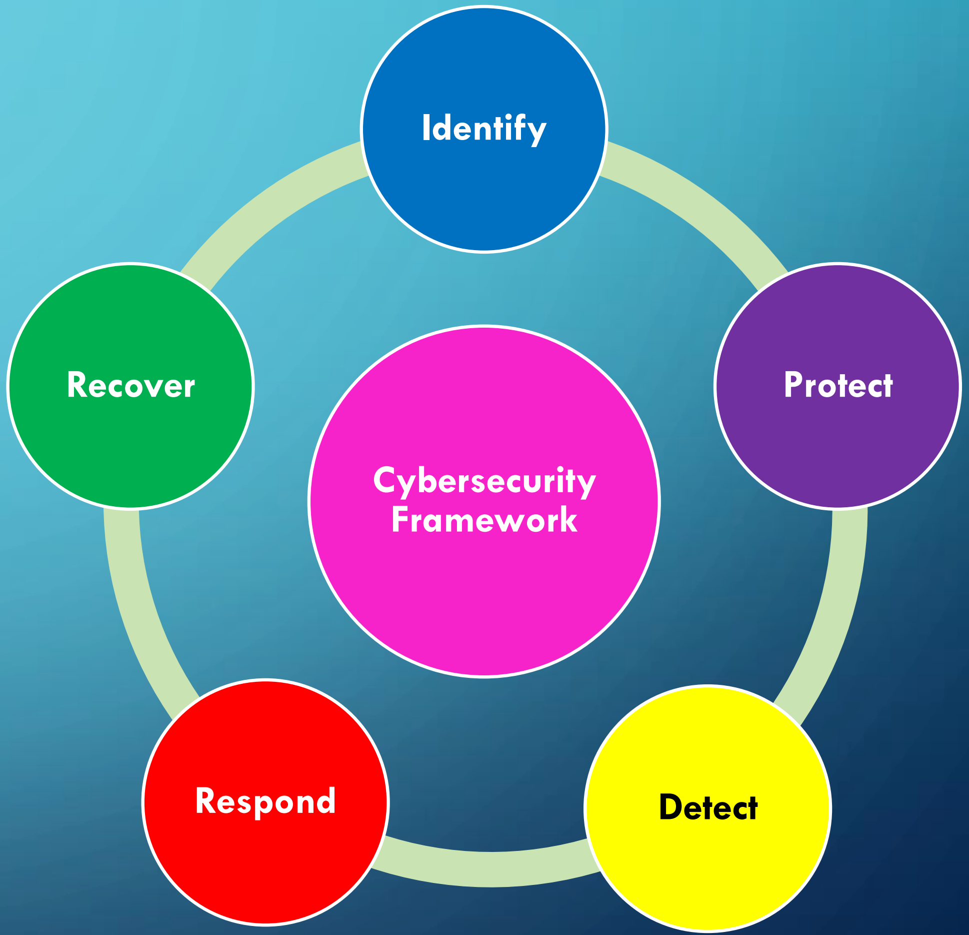
Prevention

Preparedness

Response

Recovery

Mitigation



Cybersecurity Framework

Identify

Protect

Detect

Respond

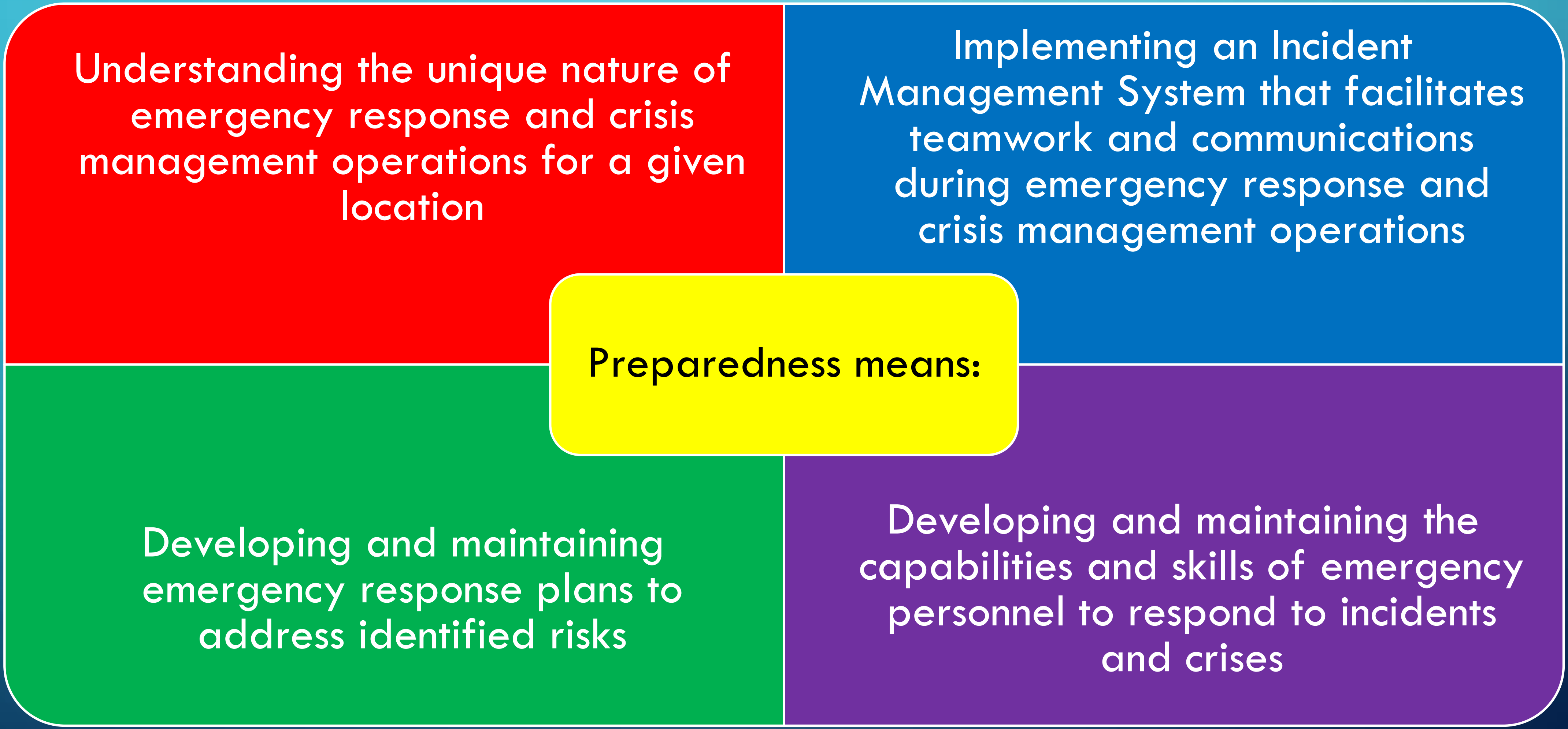
Recover

HOW I SEE EMERGENCY MANAGEMENT (PREPAREDNESS)

What do you think of when you hear the term:

“**Emergency Preparedness**”?

GOAL OF EMERGENCY MANAGEMENT – PREPAREDNESS



Preparedness means:

Understanding the unique nature of emergency response and crisis management operations for a given location

Implementing an Incident Management System that facilitates teamwork and communications during emergency response and crisis management operations

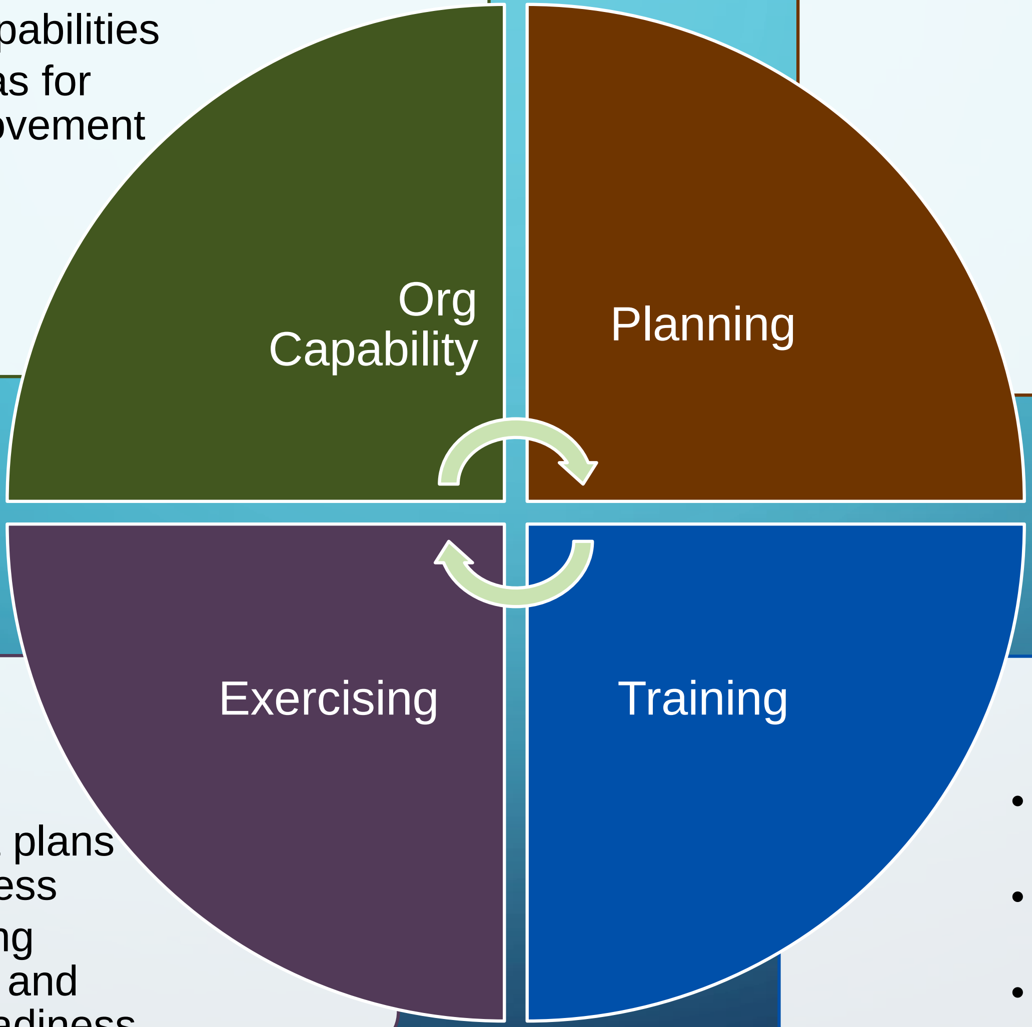
Developing and maintaining emergency response plans to address identified risks

Developing and maintaining the capabilities and skills of emergency personnel to respond to incidents and crises

EMERGENCY MANAGEMENT SYSTEM – INTEGRATED PARTS

- Evaluating key stakeholder capabilities
- Identifying areas for continual improvement

- Organizing emergency response & management teams
- Developing site & hazard-specific emergency response plans & procedures



- Evaluating procedures & plans for effectiveness
- Testing training effectiveness and responder readiness

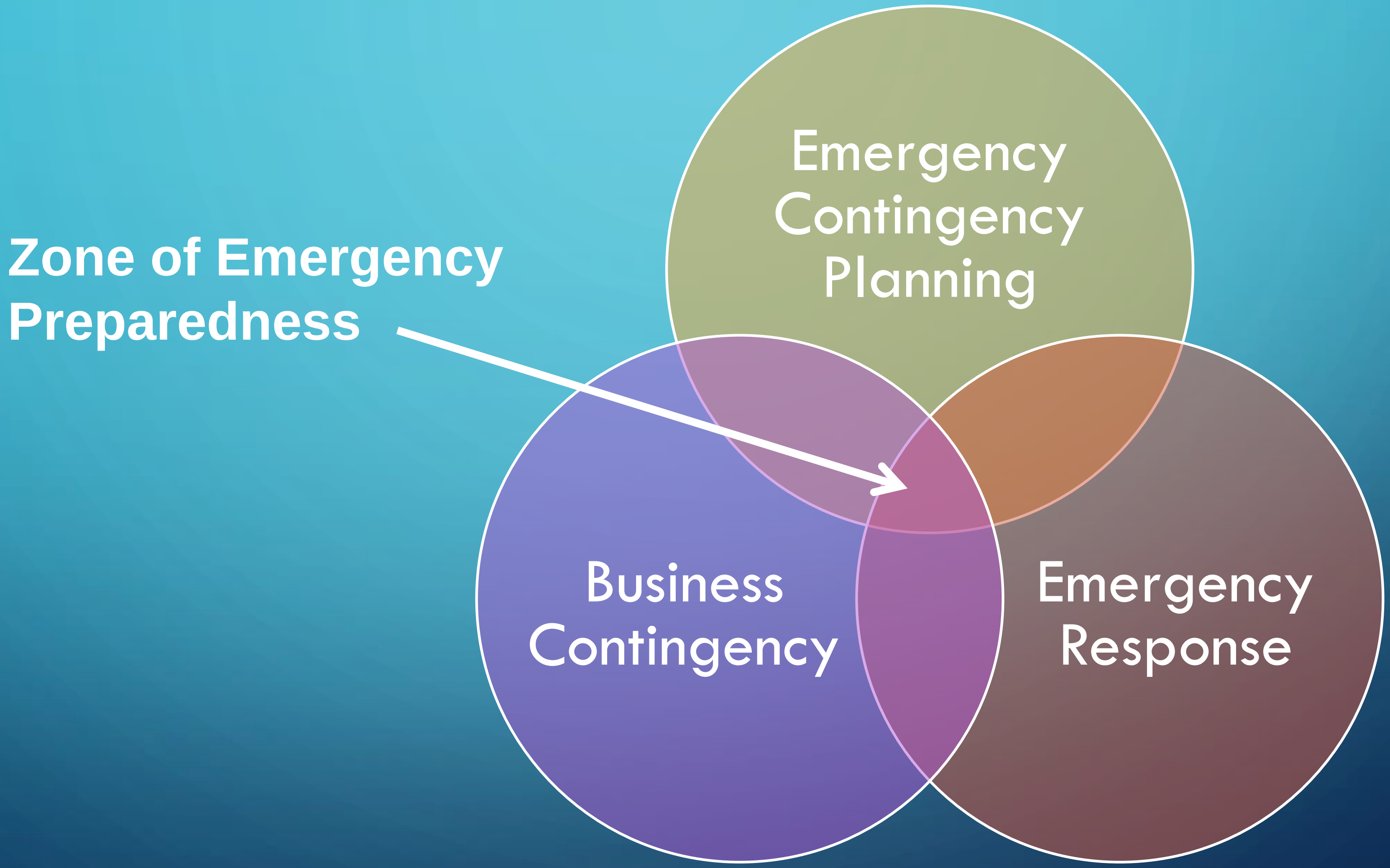
- Communicating response procedures
- Building responder competencies
- Improving responder readiness

MY VISION OF A COMPREHENSIVE EMERGENCY MANAGEMENT PROGRAM

EMERGENCY MANAGEMENT (EM) PROGRAM

Comprehensive EM Planning	*Emergency Response Organization (ERO)*	*Emergency Response Resources & Equip*	*Exercises and Training*
Risk assessment analyst Tactical/Site/Haz. Specific Response Planning ERO Planning	Tactical Response Teams EMTs CMTs BCPTs	Response Equipment Selection ICP selection and Support Inspection, Testing, Preventive Maintenance (ITPM) Program	Tactical Response Training Min. ICS training EMT, CMT, BCPT Training Annual Exercise requirements MTEP

THE SWEET SPOT



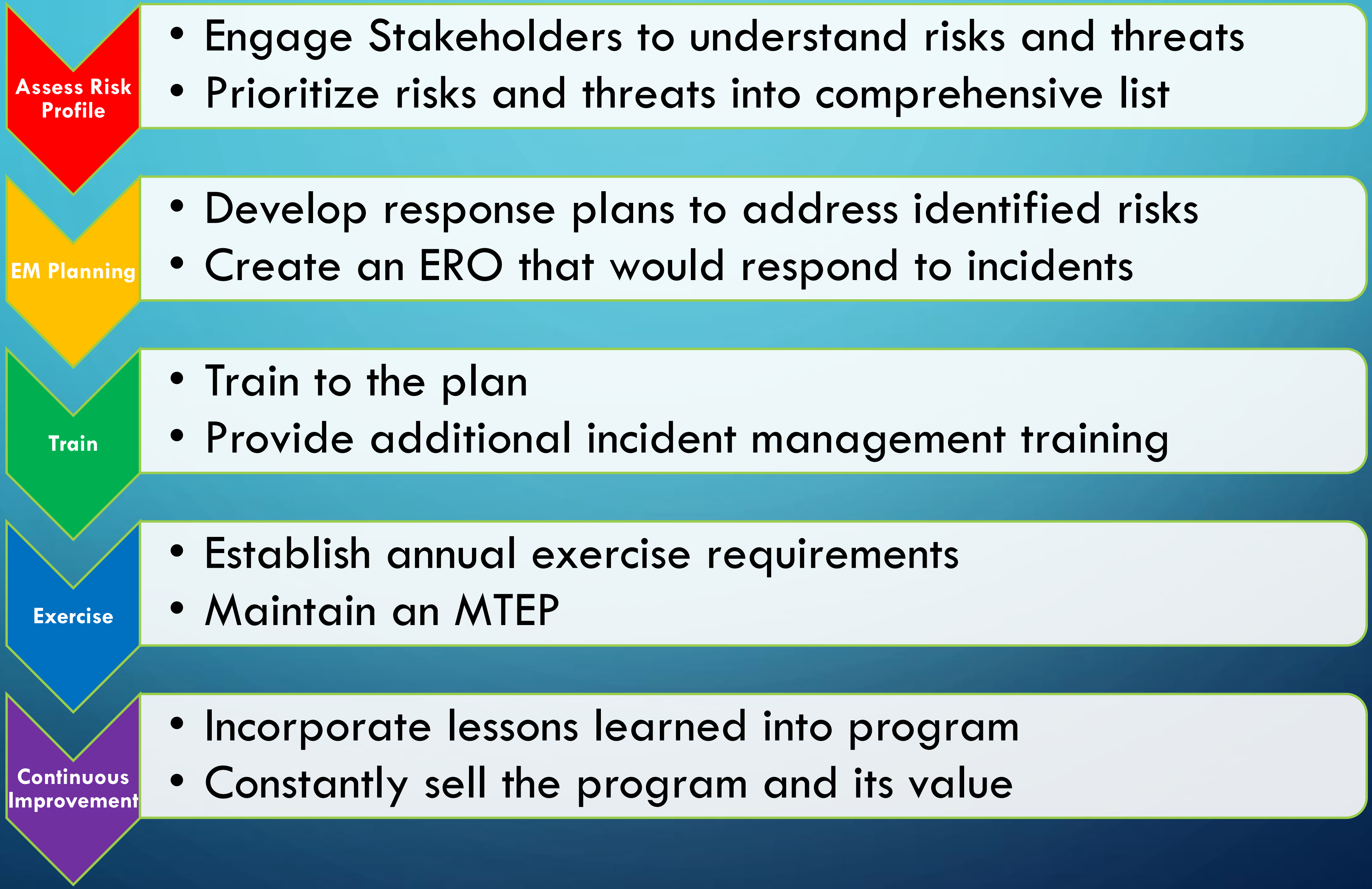
Zone of Emergency Preparedness

Emergency Contingency Planning

Business Contingency

Emergency Response

HOW I BUILD AN EMERGENCY MANAGEMENT PROGRAM



Assess Risk Profile

- Engage Stakeholders to understand risks and threats
- Prioritize risks and threats into comprehensive list

EM Planning

- Develop response plans to address identified risks
- Create an ERO that would respond to incidents

Train

- Train to the plan
- Provide additional incident management training

Exercise

- Establish annual exercise requirements
- Maintain an MTEP

Continuous Improvement

- Incorporate lessons learned into program
- Constantly sell the program and its value

INTEGRATING CYBERSECURITY INTO YOUR PROGRAM

Integrating cybersecurity into your emergency management program is no different than any other risk or potential emergency incident

Understand your agency/company's capabilities, resources, and appetite to plan and respond to cybersecurity incidents

Completely acceptable to utilize third party resources to develop and maintain your cybersecurity program; they are going to follow the same process

Not all IT professions are cybersecurity competent

ASSESS RISK PROFILE

Assess Risk Profile

If anything in your agency/company connects to the internet and or if someone can plug in a USB device, you are at risk

Know the different networks used within your agency/company

Conduct vulnerability assessments (recommend 3rd party) to determine how susceptible you are to cybersecurity incidents

EMERGENCY PLANNING

EM Planning

Use the vulnerability assessment to develop mitigation/prevention steps as well cybersecurity response plans & procedures

Due to company resources/capabilities, activities could be limited and outsourced to a 3rd party

Response plans & procedures need to be target to the right people (IT responders, EMT/CMT, end user)

TRAIN

Train

Train the right plan to the intended response group; different groups will have different responsibilities and competencies

Regular shorter engagements are better than an annual marathon session

Be open to receive and incorporate changes to plans collected from feedback during training/engagement sessions

EXERCISE

Exercise

Develop an exercise program that incorporates expectations of each response group within the organization, validation steps for response actions listed within response plans, and routine validation assessments

Recommend starting exercise program with discussion based seminars

CONTINUOUS IMPROVEMENT

Continuous Improvement

Collect lessons learned, opportunities for improvement, and all constructive feedback from engagement sessions, training, exercises and (most importantly) real incidents to improve procedures & your program

Process starts all over again to incorporate data into plans/training/exercises.

Demonstrate your program’s value to stakeholders

FINAL COMMENTS & QUESTIONS

- Integrating cybersecurity is no different that any other new risk or threat to your emergency management program
- If you have anything connected to the internet, you and your company/agency is at risk to cybersecurity incidents
- This risk will continue to increase; will start to see more physical emergencies (industrial accidents, loss of power, etc..) triggered by cybersecurity incidents
- Be careful of what you share or post online; the bad guys are watching and collecting your data

BIOGRAPHY

Over 20 years experience in emergency and crisis management for government (both Fed and State) and industry

Specialize in major oil spill response. Crisis Management and ICS instructor for Chevron

Recently served as the Asia Pacific Regional Emergency Management Advisor for Chevron; currently on a development assignment with our cybersecurity team

Currently working on my CEM and Master's in Emergency and Crisis Management

Available for corp. events and kid's parties; rballs.conference@gmail.com