Access this webinar here: https://attendee.gotowebinar.com/recording/2999617667872996111

Access speaker bios here: https://files.asprtracie.hhs.gov/documents/healthcare-cybersecurity-response-webinar-bios.pdf

Access the transcript here: https://files.asprtracie.hhs.gov/documents/healthcare-system-cybersecurity-response--experiences-and-considerations-transcript.pdf

TRACIE
HEALTHCARE EMERGENCY PREPAREDNESS INFORMATION GATEWAY

# Healthcare System Cybersecurity Response: Experiences and Considerations

March 18, 2021

ASPR
ASSISTANT SECRETARY FOR PREPAREDNESS AND RESPONSE

Unclassified//For Public Use

The opinions expressed in this presentation and on the following slides by non-federal government employees are solely those of the presenter and not necessarily those of the U.S. Government. The accuracy or reliability of the information provided is the opinion of the individual organization or presenter represented.

# ASPR TRACIE: Three Domains

**TECHNICAL RESOURCES**

- Self-service collection of audience-tailored materials
- Subject-specific, SME-reviewed "Topic Collections"
- Unpublished and SME peer-reviewed materials highlighting real-life tools and experiences

asprtracie.hhs.gov

**ASSISTANCE CENTER**

- Personalized support and responses to requests for information and technical assistance
- Accessible by toll-free number (1844-5-TRACIE), email (askasprtracie@hhs.gov), or web form (ASPRtracie.hhs.gov)

1-844-5-TRACIE

**INFORMATION EXCHANGE**

- Area for password-protected discussion among vetted users in near real-time
- Ability to support chats and the peer-to-peer exchange of user-developed templates, plans, and other materials

askasprtracie@hhs.gov

# Acknowledgements


- **Nebraska Medicine**
  - Lisa Bazis, MS
  - Brian Fox, MBA, PMP
  - Marc Ferguson, MBA, MCSM, AFBCI, CBCP
  - Shelly Schwedhelm, MSN, RN, NEA-BC
  - Dawn Straub, MSN, RN, NEA-BC
- **MedStar Health**
  - Craig DeAtley, PA-C
- **ASPR TRACIE Partners and SMEs**

TRACIE

HEALTHCARE EMERGENCY PREPAREDNESS INFORMATION GATEWAY

**Laura Wolf, PhD**
Director, Division of Critical Infrastructure Protection, HHS ASPR

ASPR
ASSISTANT SECRETARY FOR PREPAREDNESS AND RESPONSE

TRACIE

HEALTHCARE EMERGENCY PREPAREDNESS INFORMATION GATEWAY

**Moderator: John Hick, M.D.**
Hennepin Healthcare

ASPR
ASSISTANT SECRETARY FOR PREPAREDNESS AND RESPONSE

# Setting the Stage

- Focus on effects of cyber incidents on the healthcare operational environment, specifically:
  - Ability to effectively care for patients
  - Maintaining business practices
  - Ensuring readiness and recovery
- Cyberattacks were identified as top threat in healthcare system Hazard Vulnerability Analyses (HVAs)
- Lessons learned and best practices should be shared across the health sector to improve preparedness and response efforts

# Select Cybersecurity Resources

- ASPR TRACIE
  - Cybersecurity Topic Collection
  - Exchange Issue 2: Cybersecurity and Cyber Hygiene
  - Cybersecurity and Healthcare Facilities Video
  - Healthcare System Cybersecurity: Readiness and Response Considerations and accompanying Overview Presentation
- ASPR
  - ASPR Critical Infrastructure Protection
  - Health Sector Cybersecurity Coordination Center (HC3)
  - Joint HPH Cybersecurity Working Group/405(d) Program

TRACIE

HEALTHCARE EMERGENCY PREPAREDNESS INFORMATION GATEWAY

**Craig DeAtley, PA-C**
Director, Institute for Public Health Emergency Readiness,
MedStar Washington Hospital Center

ASPR
ASSISTANT SECRETARY FOR PREPAREDNESS AND RESPONSE

# Opening Thoughts

- IT CAN HAPPEN TO YOU!!
- It should be on everyone's HVA
- A planning committee is an important starting point
  - Multidisciplinary representation
  - External partners/vendors
  - System representation on a facility committee and vice versa are critical to success on both sides
  - Meet regularly
  - Take notes

# At the Start

- Spend some time learning about past attacks
  - What happened and how?
  - Do those vulnerabilities relate to your facility/organization?
  - What lessons learned pertain to you?
- The Incident Response Plan should be comprehensive and not just a compendium of individual downtime practices
  - Alert /notification/authorities
  - Incident Management Team
  - Business Continuity/Business Impact Analysis
- Understand what will be enterprise-wide practice/decision versus local practice/opportunity for planning and response

# Critical Preparedness Next Steps

- Maintain a list of all of your applications
  - Ensure new applications are added and they include downtime procedure and recovery steps
  - This includes biomedical equipment/ phones/ infrastructure controls
  - Keep back up copies!!
- Ensure that you understand how each application relates to one another
  - If you have links with external partners (e.g., HCC) keep them current
  - Make sure updates, patches, etc. are done on a timely basis

# More Points on Preparedness

- Consider an external audit committee to assist with planning input and guidance
- Establish a priority restoration plan – can't bring them all back at once
- Don't focus just on clinical impact of an outage
  - Gift shop, parking, security, cafeteria, HR, payroll, etc.
  - Revenue cycle impact
- Practice, Practice, Practice!!!
  - But how?!!

# Important Response Steps

- Have a clear problem reporting process
- Have clarity on definitions and who has authority to initiate the plan(s) and escalation procedures
- Duplication of alerting systems is important
- Consider having “Go Bags” containing critical items (e.g., plans, forms, checklists, etc.)

# Additional Response Steps to Consider

- Communication will be critical – how can it best be done?!
- 24/7 IMT staffing and Unit/office downtime expertise will be needed along with Just-in-Time Training
- Address written record security and archiving
- Can we still provide high quality and safe patient care?
- Share updated work arounds/situational awareness for each shift

# Additional Response Steps to Consider, con't

- What about the Health Information Exchange – can it be accessed and used?
- Redeploy staff to needed areas
  - Pharmacists to busy units
  - Staff who can't otherwise do their job – runners, scribes
- Work from home is an option
- Safety officer(s)/ security officers/ trainers roving

# Recovery is Vital, too!!

- Planning for it starts early
- Dedicate staff to planning and executing this phase
- What are vendors doing?
- Implement the restoration priority list – and prepare for issues
- Communicate, communicate, communicate!!
- Data entry will be tedious, tiring, and labor intensive

# Finally…

- Some data may/not be reconcilable
- Some IT applications may/not become non-recoverable
  - More likely when they are not part of the planning and recovery effort
- Financial implications should be expected so record them – from the outset and work with insurance company to address
- Public messaging will be important all along – but what can be said and who should say it may not be as easy as you think
- Effective communications (not just the plan) is important

TRACIE

HEALTHCARE EMERGENCY PREPAREDNESS INFORMATION GATEWAY

**Dawn Straub, MSN, RN, NEA-BC**
Executive Director, Nursing Professional Practice & Informatics,
Nebraska Medicine

ASPR
ASSISTANT SECRETARY FOR PREPAREDNESS AND RESPONSE

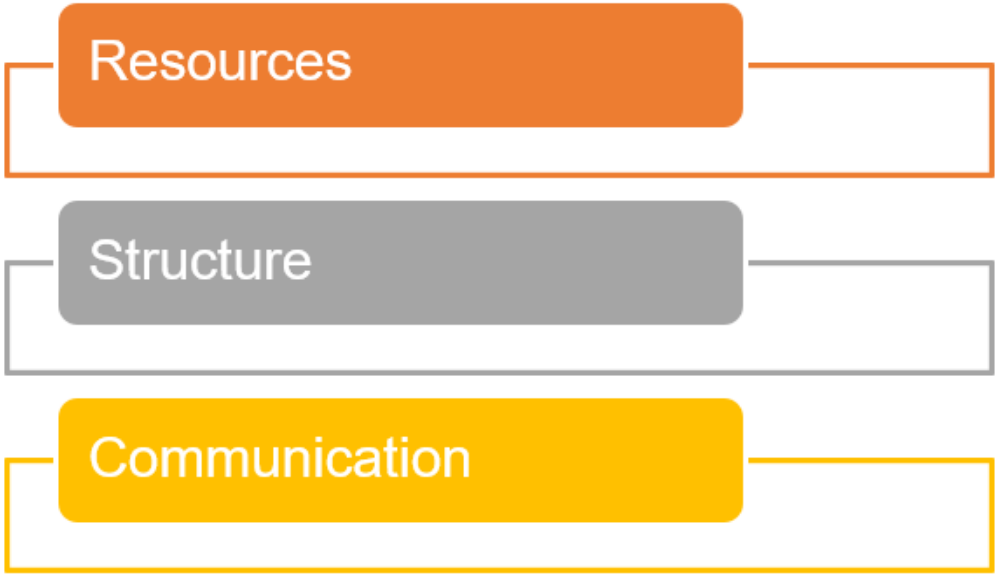
# Operational Perspective


**FEMA Emergency Management Cycle**

# Prepare - The Mindset

- The question is not “if” this will happen but “when”…
- Cyber hygiene is a patient safety goal

# Prepare - HICS Training



# Prepare - Resources

**ALL departments must have business continuity plans**

- Downtime preparedness checklist
- Systematic, on-going teams and preparedness processes
- Channels for approval and updates
- Drill, drill, drill

# Prepare

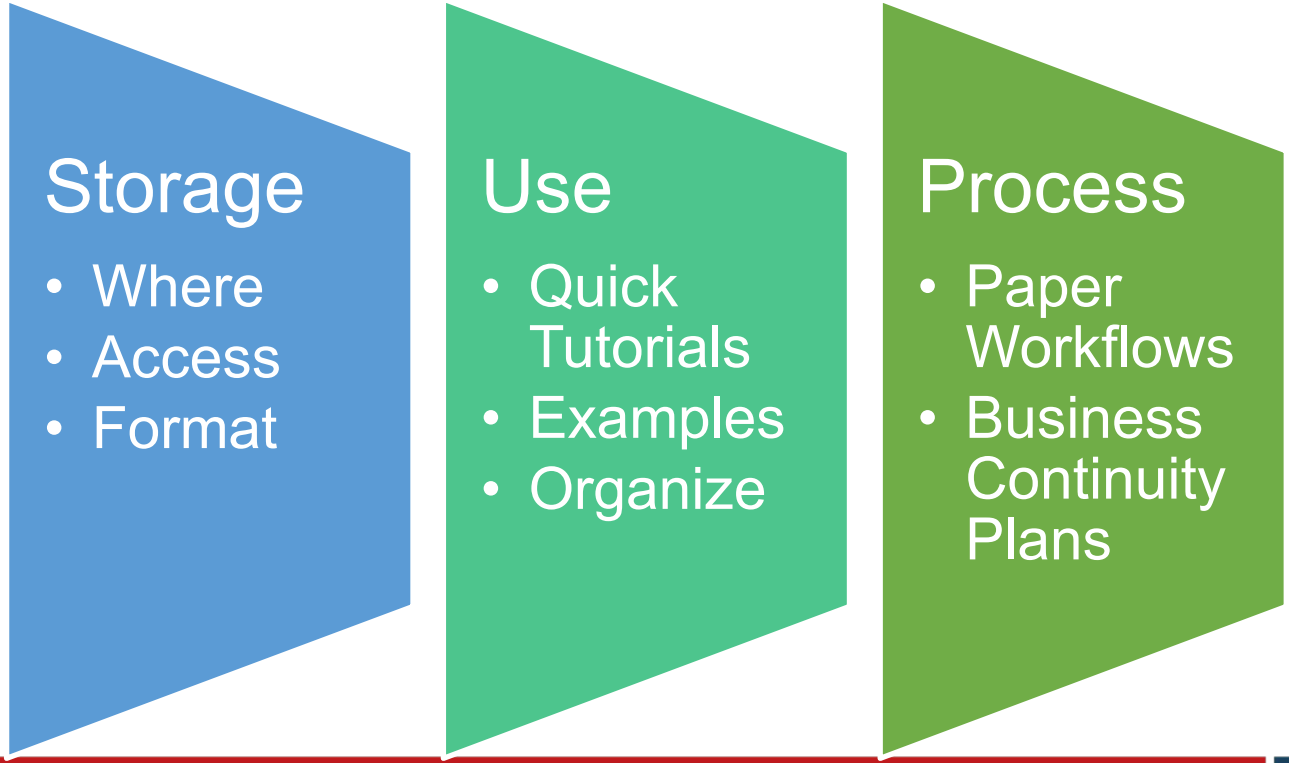
- ❑ Validate that your unit "Go Bags" are ready


**Unit "Go Bag" Contents:**

- ✓ Flashlights/Headlamps- check batteries
- ✓ White stickers with unit name on them (e.g., 6West) Unit evacuation plan
- ✓ Unit smoke compartment map
- ✓ Unit severe weather plan
- ✓ Unit fire/evacuation plan
- ✓ Both Severe Weather Checklists (Lead RN and RN-Clerk Tech-*need several copies)
- ✓ Pens, paper, clipboards
- ✓ Red, Yellow, Green arm bands (only use when you need to leave the floor via the stairwells)
- ✓ Unit supplies (e.g., masks, basins, tape, gloves, etc.)

- ❑ Review the checklists with Lead(s) & Staff
- ❑ Pull out the medsled and practice
- ❑ Check flashlights and headlights and CHANGE BATTERIES
- ❑ Participate in drill(s): Wed. March 28th – 1000 & 2000
- ❑ Provide feedback via electronic drill survey

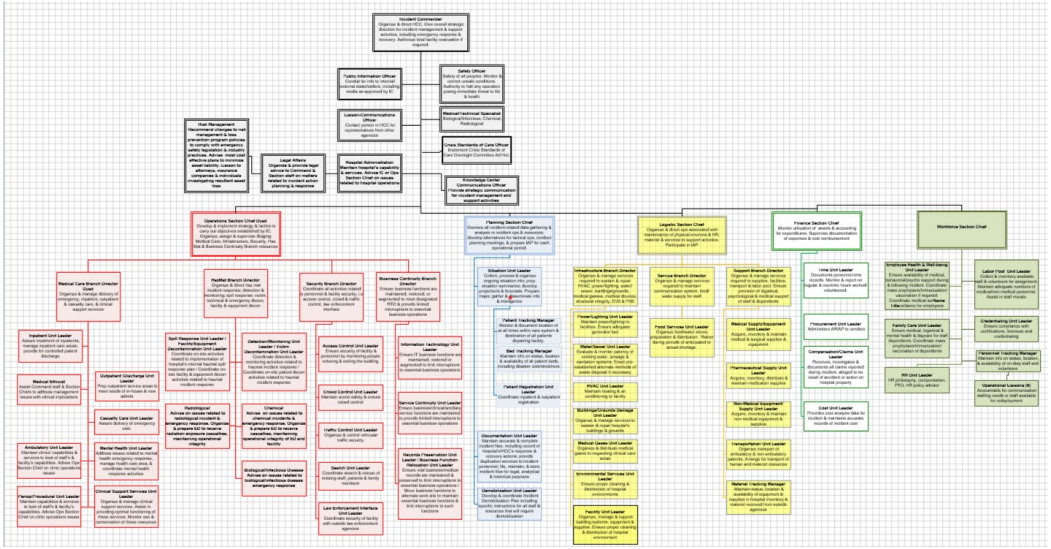
# Prepare - Forms



# Response - Implement

HICS

- Define critical services
  - Systems affected
  - Length of downtime
- Clinical Promising Practices – pg. 22



# Response - Implement

**Communicate, communicate, communicate!!**

- Consider informatics team to assist with translation of clinical/operational staff and IT staff
- Use structure to assist with internal messaging
- Assign specific resources to external communication

# Response - Workforce

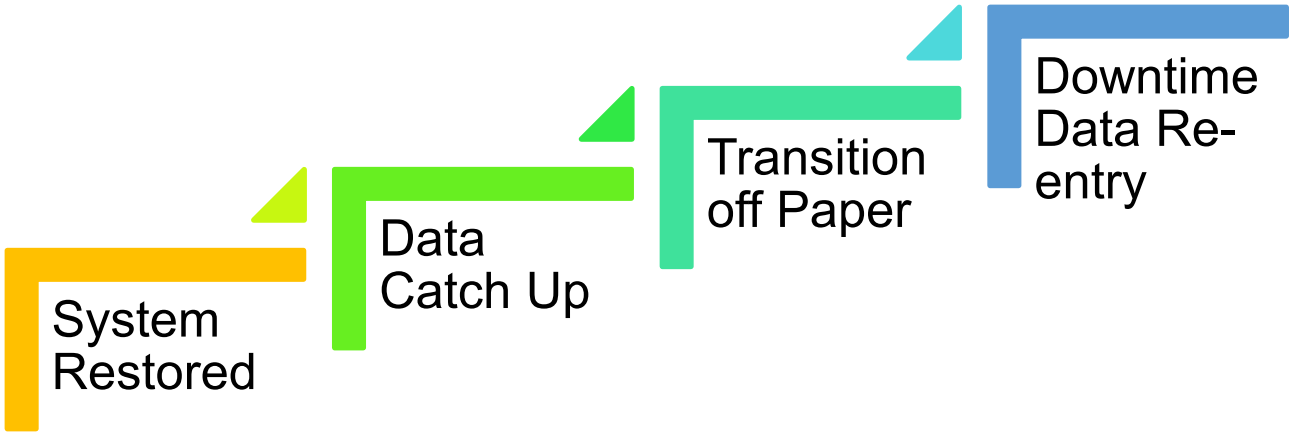
## All hands on deck

- Assign leaders with calm, cool approach
- Consider unit/department deployment for lab, pharmacy, coders
- At the elbow assistance on units
- Those who cannot work can be helpful elsewhere
  - Runners

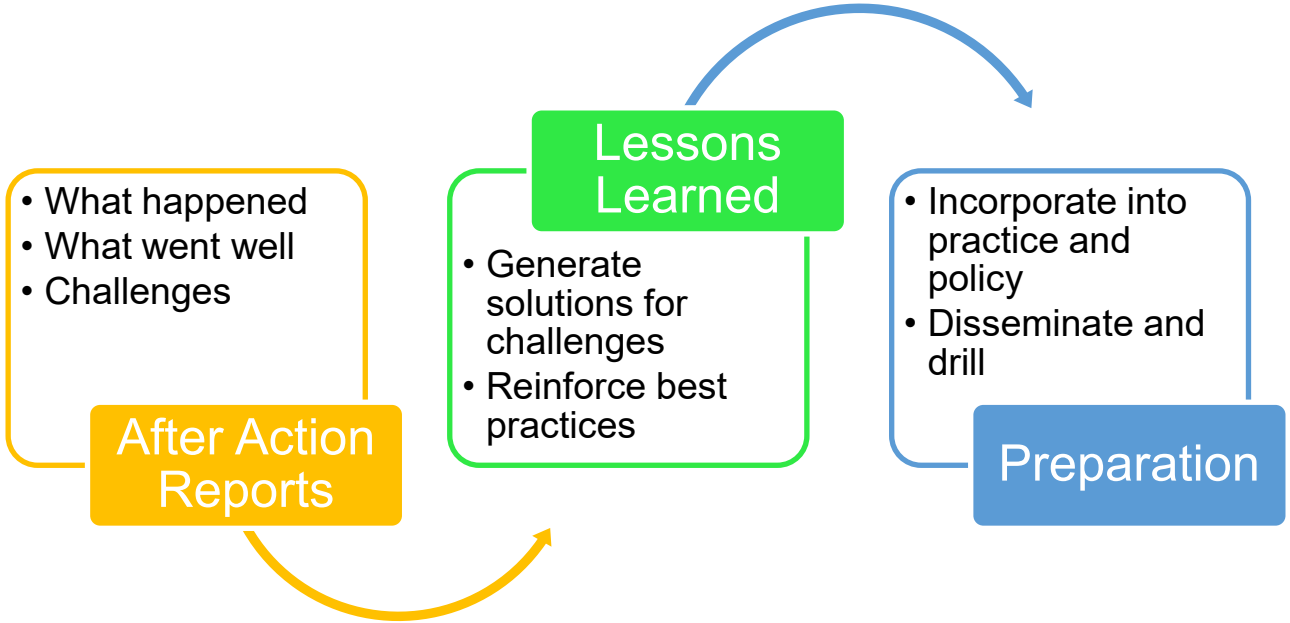
# Recovery

**Communicate, communicate, communicate!!**

- Marathon
- Dimmer Switch Approach



# Mitigation


• What happened
• What went well
• Challenges
After Action Reports
Lessons Learned
• Generate solutions for challenges
• Reinforce best practices
• Incorporate into practice and policy
• Disseminate and drill
Preparation

TRACIE

HEALTHCARE EMERGENCY PREPAREDNESS INFORMATION GATEWAY

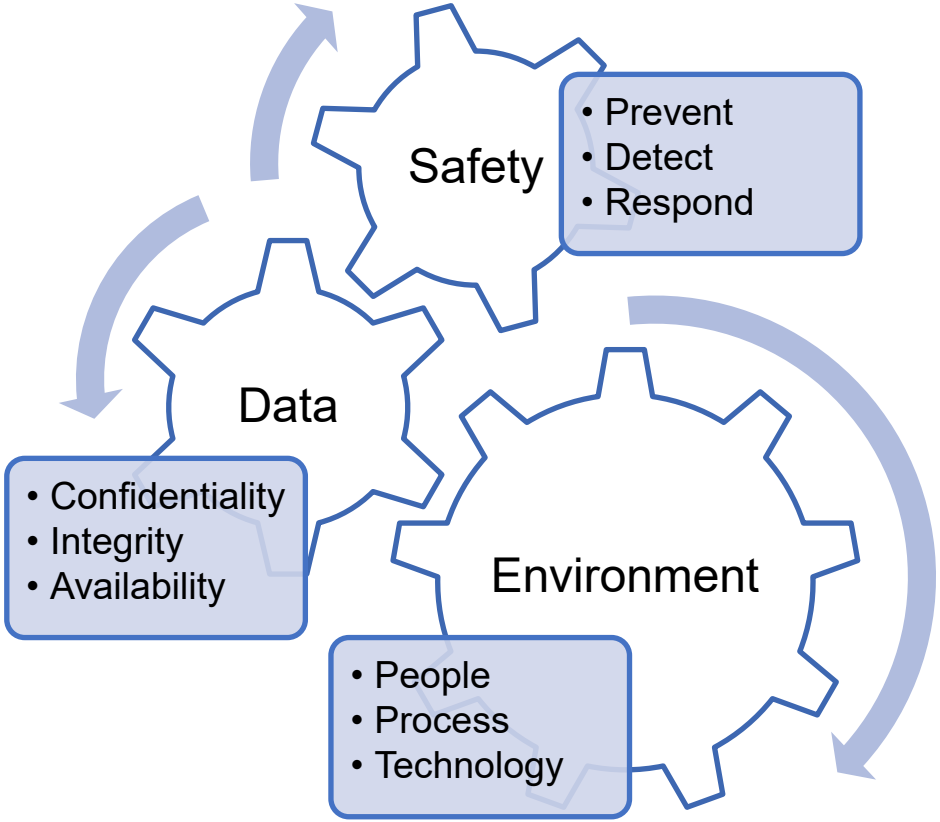
**Lisa Bazis, MS**
Chief Information Security Officer, Nebraska Medicine

ASPR
ASSISTANT SECRETARY FOR PREPAREDNESS AND RESPONSE

# Cyber Security – Not just an IT issue


Trust
Accountability
Empowerment


- Understand
- Know
- Learn
- Recover


Safety
• Prevent
• Detect
• Respond
Data
• Confidentiality
• Integrity
• Availability
Environment
• People
• Process
• Technology


SECURI
RECOVERY
RESILIENCE
CONTINGENCY
BUSINESS
OPERATE
PLANNING
INCIDENT
CONTINUITY
MANAGEMENT
ROCEDURES
RISK
ORGANIZATION
PLAN
PREPARATION
ANDARD
DISASTER

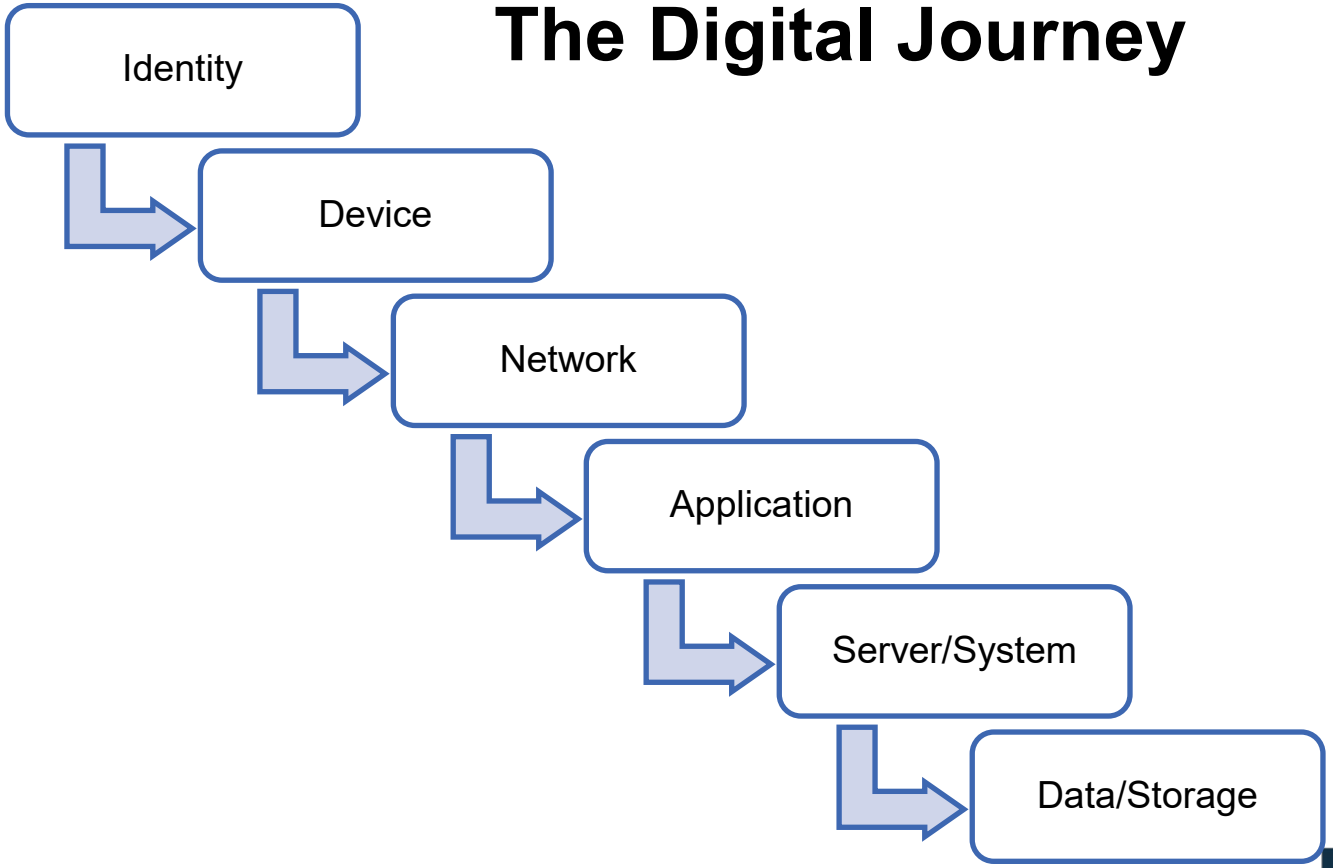
# How to Build Business Continuity

- Application/System Inventory & Interconnections
  - Know the technical & business owners
- Application Business Value Rating (ABVR)
- Drills/Exercises/Downtimes

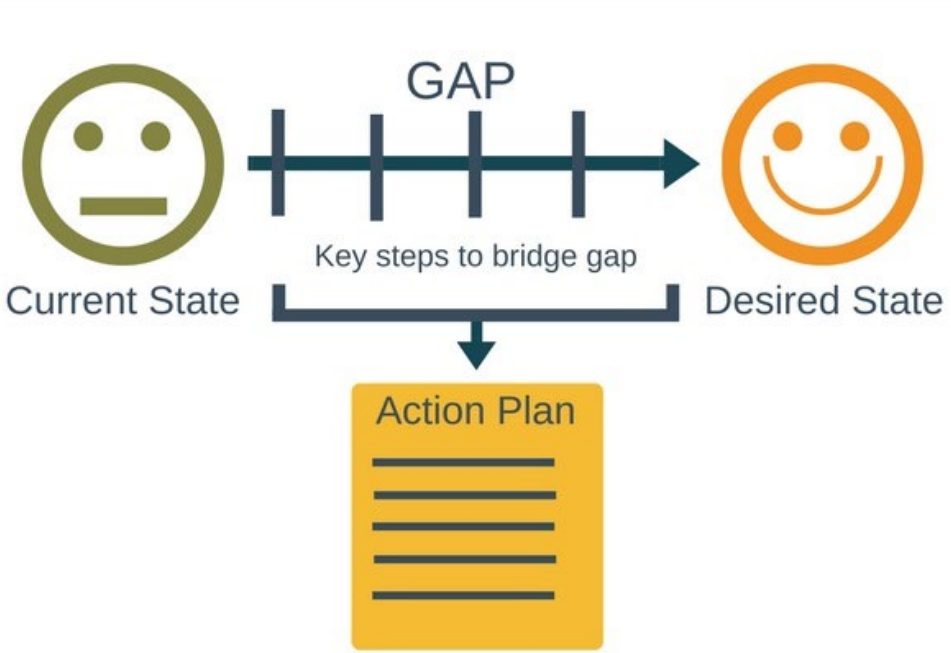
# How to Handle the Fire

- Protect
- Detect
- Suppress
- Contain
- Restore

# The Digital Journey



# Create the Gap Assessment



# Positive Outcomes

Safety

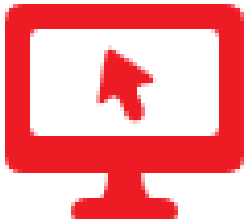
Business

Reputation

Board Of Directors

# Question & Answer

# Contact Us



asprtracie.hhs.gov

1-844-5-TRACIE

askasprtracie@hhs.gov