# DISASTER PREPAREDNESS

Lunch and Learn Series

Beckie Gierer, Director,
Missouri Department of Mental Health

MISSOURI DEPARTMENT OF HEALTH & SENIOR SERVICES

Missouri Department of MENTAL HEALTH

# DISASTER PREPAREDNESS AND EMPLOYEE WELL-BEING

Disasters—whether natural or man-made—can disrupt lives, workplaces, and communities in an instant. They can be overwhelming, frightening, and deeply destabilizing. Understanding how disaster preparedness connects to trauma, resilience, and employee well-being helps organizations build cultures of safety, trust, and stability.

Preparedness isn't just a logistical necessity—it’s a preventive well-being tool. When people know what to expect, where to go, and how to respond, they experience less uncertainty and stress. A trauma-informed approach to disaster preparedness supports both individual and collective resilience, helping employees feel more grounded and capable when challenges arise.

# WHY DISASTER PREPAREDNESS MATTERS IN A TRAUMA-INFORMED

Disasters can have significant emotional and psychological impacts. A trauma-informed workplace recognizes that:

- Everyone will experience a disaster differently
- Past experiences shape how people respond
- Stressful events can trigger a wide range of reactions
- Safety, predictability, and communication reduce retraumatization

Trauma-informed disaster preparedness means understanding these reactions and responding in ways that support people—not overwhelm them.

# HOW PREPAREDNESS SUPPORTS EMPLOYEE WELL-BEING

**Preparedness reduces stress before, during, and after an event. When employees know:**

- The plan
- Their role
- How to care for their families
- Where to go and what steps to take

**...they are less likely to experience panic, confusion, or decision paralysis during an emergency.**

**Being prepared doesn't remove all stress—but it significantly lessens the burden and helps people stay focused, anchored, and safer.**

**Preparedness also reinforces a well-being culture. When organizations invest in readiness, employees feel valued and protected, which boosts trust, psychological safety, and overall morale.**

# BUILDING A CULTURE OF SAFETY, TRUST, AND BELONGING

> Disaster preparedness becomes part of the workplace culture when it's reinforced early and often.

**This includes:**

- **New employee orientation** that covers emergency plans and expectations
- **Clear communication** about where to go, who to contact, and what roles employees have
- **Regular training** and drills to help people practice response steps
- **Inclusive discussions** that allow employees to ask questions and build confidence

**When preparedness is integrated from day one, employees feel safer, more supported, and more connected to their organization.**

**This proactive approach builds belonging and reduces the anxiety that comes with uncertainty.**

# WHAT DISASTER SERVICES DOES (AND HOW THEY SUPPORT WELL-BEING)

An effective disaster response system involves preparation, coordination, and ongoing support. Disaster service teams often work with:

- Local partners: emergency managers, nonprofits, and community providers
- State and federal partners: agencies involved in public health, emergency management, and behavioral health
- Community members: individuals and families affected by disasters

Their works include:

## Planning and Preparedness

- Developing emergency plans
- Conducting drills and exercises
- Training employees and community partners
- Teaching psychological first aid and coping strategies

## Response and Recovery

- Deploying behavioral health teams to provide crisis counseling
- Supporting individuals, families, and communities in the immediate aftermath
- Offering referrals and additional mental health resources
- Ensuring a coordinated mental health response during and after disasters

These services help reduce long-term trauma, strengthen community resilience, and support recovery in a holistic, trauma-informed way.

## Accessing Disaster Support

Workplaces and community members can connect with disaster services through:

- Organization websites and contact forms
- Listed phone numbers for disaster support teams
- Local emergency management agencies
- State emergency management agencies
- Public health departments
- Direct outreach in urgent situations

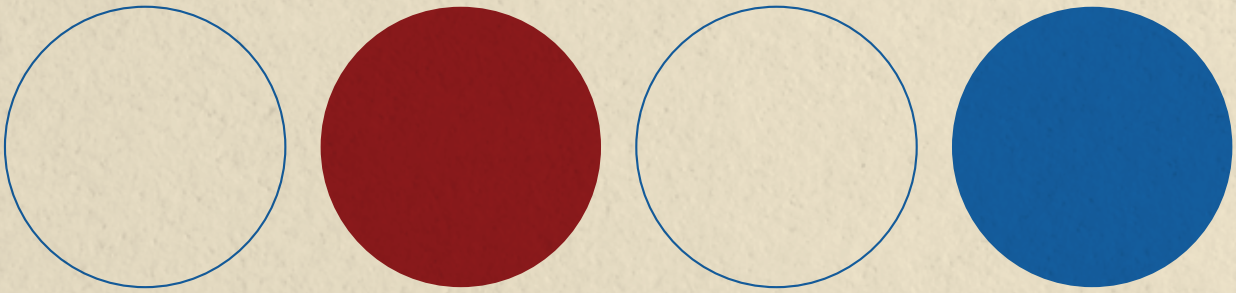
Rapid access to support ensures timely deployment of behavioral health strike teams and helps stabilize affected individuals and communities.

# MOVING FORWARD: BUILDING RESILIENCE TOGETHER

Disaster preparedness is a critical part of creating trauma-informed, resilient workplaces. When organizations invest in planning, education, and coordinated response, they foster a culture where employees feel safe, supported, and empowered.

Preparedness not only protects physical safety—it strengthens emotional well-being, team cohesion, and long-term resilience.

By preparing together, workplaces can not only bounce back from challenges—they can bounce forward, emerging stronger, more connected, and more capable of supporting one another through whatever comes next.



# SCENARIO: CYBER ATTACK

## Day 1

**The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) Health Sector Cybersecurity Coordination Center (HC3) release a joint alert regarding a rise in cyberattacks targeting healthcare organizations. The alert describes the tactics, techniques, and procedures (TTPs) used by cyber criminals, including phishing emails, ransomware, remote hacking, distributed denial of service (DDoS) attacks, and data exfiltration from healthcare organizations.**

## Day 3

**Employees receive email notifications to update their work profile. The email contains fake reCAPTCHA prompt where the user will click to verify if they are human and then to copy the command to their clipboard and instructs them to press Windows+R, past the command and run it. This leads to the download of various malware.**

## Questions:

- What are the greatest cyberthreats to our organization?
- What cybersecurity information do you receive from the organization?
- What is our organization's cybersecurity practice? (How frequently do we get prompted to change passwords? Do we use multi-factor authentication?)
- What would you do in this situation if you discovered your computer has malware downloaded?

## Day 7

**Ransomware messages appear on computers throughout the agency and users report they are unable to access their files. You open your computer and notice your files all have different names. A message is displayed that reads:**

**“Hello! Your files have been held hostage. We have your data. But do not fear because for the sum of $1,000,000 (9.8 BTC/3/25) your files will be returned. The decryption key will expire in 72 hours. Please submit payment to the wallet below or we will start selling data to the highest bidder.”**

**Now, all devices are down, including those connected to the internet.**

## Questions:

- How have your priorities changed based on these current events?
- If your phones are internet based, how will you reach your supervisor?
- Does every team member have numbers programmed/written down to contact our team in the event phones are down?
- Has each team member registered for Groupcast?
- Does each WTWS know who to contact in their office setting?