THA Summer Conference

# YOU'VE BEEN HACKED. NOW WHAT?

## Responding effectively to a cybersecurity crisis

FTI CONSULTING

September 2025

# AGENDA

1. Today's Cyber Threat Landscape
2. Effective Communications Response
3. Bringing it to Life: *Panel Discussion*

# Today’s Cyber Threat Landscape

# By the Numbers


Change cyberattack serves as wake-up call for healthcare cybersecurity

The outage shows why health systems need to plan for inevitable cyberattacks, evaluating risks to their operations and financials and putting backups in place, experts say.

Published April 4, 2024


By the numbers: The impact of the Ascension cyberattack

The health system, one of the largest nonprofits in the country, lost access to its electronic health record, patient portal and some phone systems after the attack in early May.

Published June 17, 2024


MATT BURGESS SECURITY JUN 24, 2024 5:00 AM

Red Tape Is Making Hospital Ransomware Attacks Worse

With cyberattacks increasingly targeting health care providers, an arduous bureaucratic process meant to address legal risk is keeping hospitals offline longer, potentially risking lives.


Kettering Health confirms cyberattack involves ransomware, calls incident 'jarring'


Systems Now Online at Lurie Children's Hospital Following January Cyberattack

Posted By Steve Alder on May 27, 2024

**181** The number of confirmed ransomware attacks on healthcare providers; **five of the top 10 ransomware attacks in 2024 were on healthcare organizations**
*Source: Comparitech*

**$21.9B** The amount healthcare organizations have **lost to downtime alone** as a result of ransomware attacks since 2018
*Source: Comparitech*

**185M** The approximate number of breached healthcare records in 2024, **the worst-year ever on record**
*Source: U.S. Department of Health and Human Services' Office for Civil Rights*

**55%** The percentage of hospital executives who **admit they are not very prepared** for a cyberattack
*Source: FTI Consulting U.S. Healthcare & Life Sciences Outlook 2024: Hospital Operations Survey*

# Evolving Trends & Threats

## Attacks Targeting Supply Chains

Threat actors are successfully infiltrating "target rich" organizations that operate global supply chains.

## Vendor Breaches & Third-Party Incidents

Companies face a greater risk from exposure to third parties than ever before.

## Increased Regulation

Governments around the world continue to refine policies and protocols with respect to critical infrastructure.

## AI & Social Engineering

Threat actors have more tools and methods at their disposal to try and gain entry into a company's systems.

## Aggressive Extortion Tactics

Emerging extortion tactics present risk to physical safety, such as swatting and death threats against executives.

# The Realities




6

# Effective Communications Response

FTI CONSULTING

# A Team Sport

## Legal

- Retains incident response vendors under privilege
- Coordinates with law enforcement and regulators
- Reviews communications materials for legal risk

## Information Security

- Determines scope and root cause of incident
- Implements remediation measures
- Provides input into communications materials

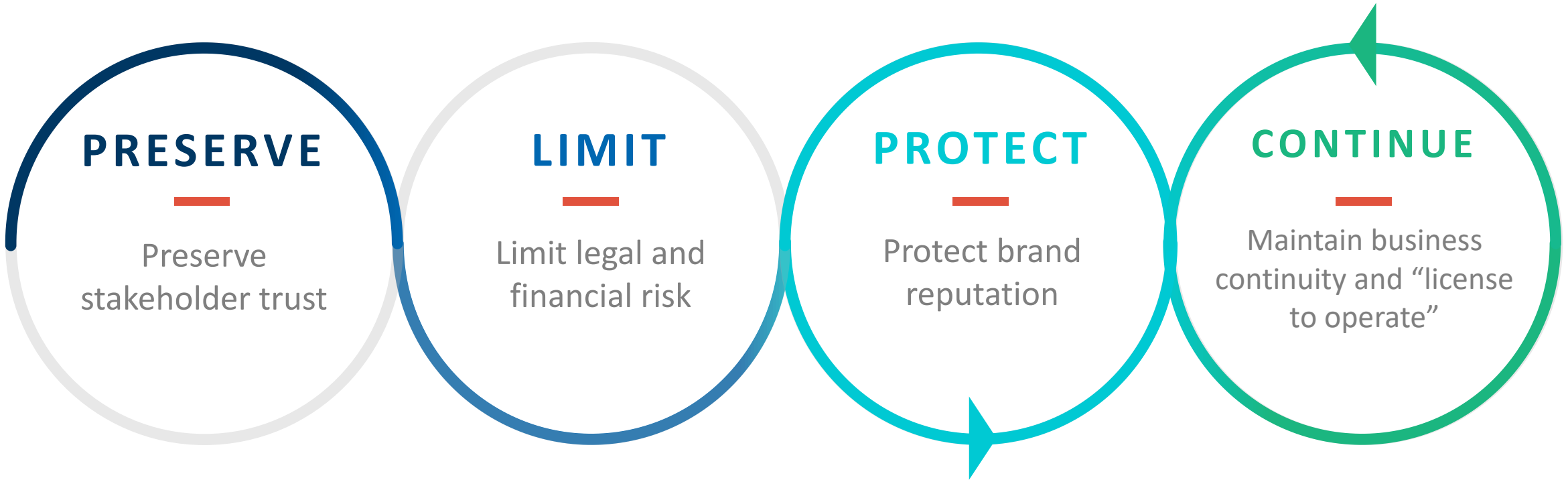
## Operations

- Focuses on recovery of systems
- Establishes workarounds for continuity of care
- Provides points of progress for messaging

## Communications

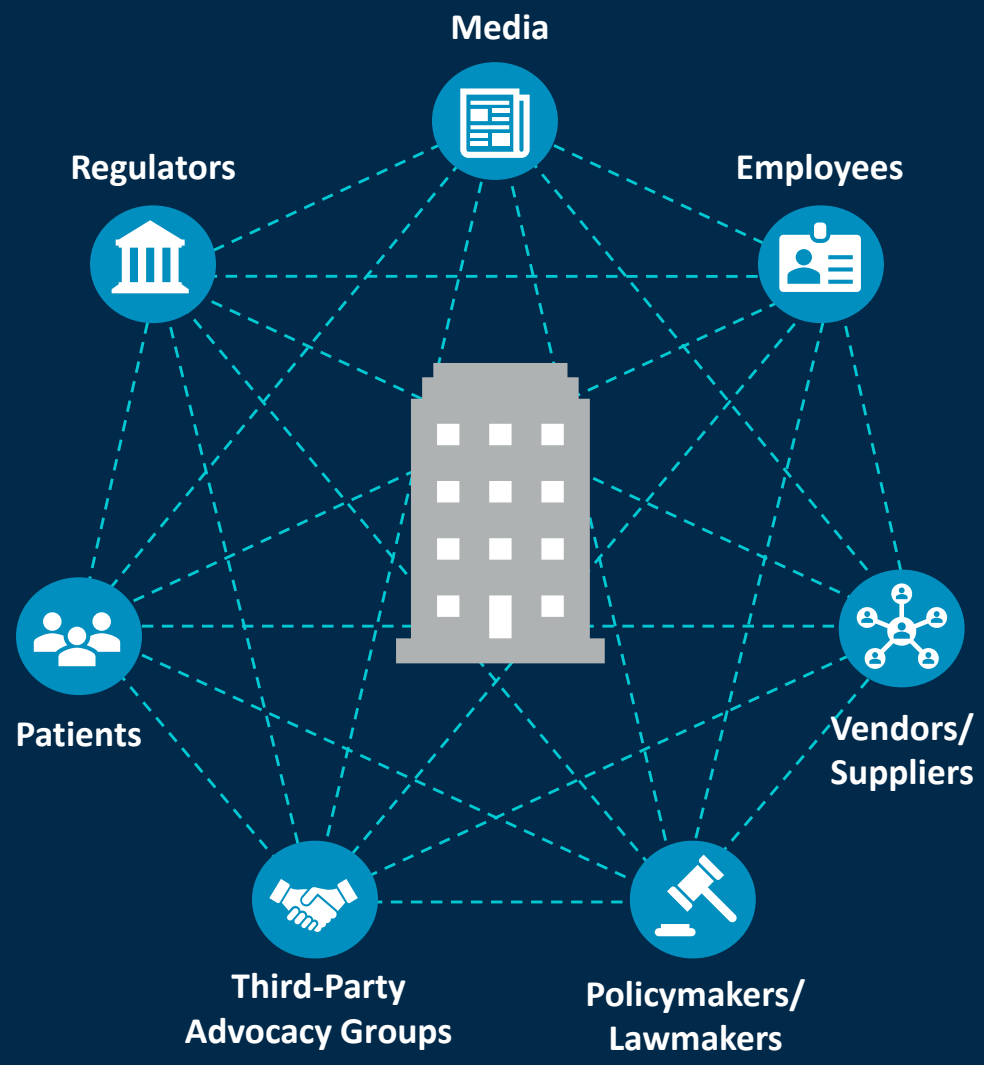
- Develops core messaging
- Establishes multi-stakeholder communications plan
- Focuses on mitigating reputational risks

# The Role of Communications in Incident response



# Stakeholder Mapping

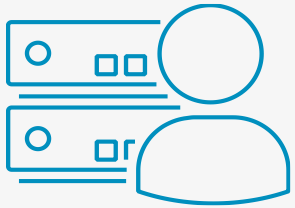
- Anticipate an influx of stakeholder inquiries
- Know that specific information is not always available – both immediately after and in the weeks following
- Address misinformation/ rapidly and effectively



# Communications Best Practices

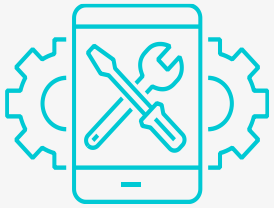
## Responsiveness

*Communicate actionable information to all stakeholders*



## Accuracy

*A communications strategy is only as good as the facts on the ground*



## Transparency

*Convey honesty, while also balancing transparency and risk*

## Consistency

*Consistency in message across stakeholder groups is key*

# Lessons Learned

# Common Pitfalls to Avoid

**01** Operating in siloes

**02** Getting ahead of the facts

**03** Neglecting internal communications

**04** Underestimating the volume and range of stakeholder inquiries

# KEY TAKEAWAYS

**01** Establish a “Single Source of Truth”

**02** Anticipate key inflection points

**03** Establish relationships with key vendors/partners in advance

**04** Adopt a preparedness mindset

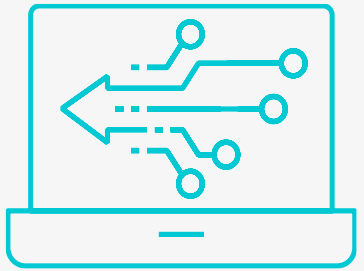
# How Your Organizations Can Best Prepare Today

## Assess Existing Infrastructure

- Ensure alignment among business continuity, cyber incident response and crisis communications plans
- Update plans to reflect the latest threats
- Explore out-of-band/off-network communications channels

## Refine Your Plan

- Outline roles and responsibilities, decision maker for a cyber incident
- Document comms approval process
- Scenario plan in advance



## Practice Makes Perfect

- Utilize tabletop exercises and simulations to build muscle memory
- Focus on downtime procedures and comms challenges
- Continuously update… security is never over!

# Panel Discussion

**Janelle Reilly**
*Market Chief Executive Officer*
*CHI Memorial*

**Matt Schaefer**
*President and CEO*
*East Tennessee Children's Hospital*