99TH NHA ANNUAL Convention

SCAN HERE

Responding Effectively to Cybersecurity Incidents

Jamie Singer
Senior Managing Director
FTI Consulting

NHA | NEBRASKA HOSPITALS

FTI Consulting Cybersecurity & Data Privacy Communications

Responding Effectively to Cybersecurity Incidents



Agenda

1. Cyber Landscape in Healthcare
2. Communications Response and Preparedness Best Practices
3. Bringing it to Life: *Scenario Run-Through*
4. Key Takeaways

Cyber Landscape in Healthcare

By the Numbers

Change cyberattack serves as wake-up call for healthcare cybersecurity

By the numbers: The impact of the Ascension cyberattack

72% of healthcare organizations say cyberattacks caused care delays, longer hospital stays

Oracle Health breach compromises patient data at US hospitals

University of Mississippi Medical Center Restores Epic EHR System After Major Ransomware Attack and Nine-Day Clinic Closure

293

The number of ransomware attacks recorded on hospitals, clinics, and other direct care provider in the first nine months of 2025

Source: Comparitech

$21.9B

The amount healthcare organizations have **lost to downtime alone** as a result of ransomware attacks since 2018

Source: Comparitech

42.5M

The approximate number of people impacted in 2025 by cyberattacks in healthcare

Source: U.S. Department of Health and Human Services' Office for Civil Rights

47%

The percentage of healthcare leaders who **believe their organizations are vulnerable to a cyber incident**

Source: FTI Consulting Survey: U.S. Healthcare & Life Sciences Industry Outlook 2026

Evolving Trends & Threats

Attacks Targeting Supply Chains	Vendor Breaches & Third-Party Incidents	Increased Regulation	AI & Social Engineering	Aggressive Extortion Tactics
Threat actors are successfully infiltrating "target rich" organizations that operate global supply chains.	Companies face a greater risk from exposure to third parties than ever before.	Governments around the world continue to refine policies and protocols with respect to critical infrastructure.	Threat actors have more tools and methods at their disposal to try and gain entry into a company's systems.	Emerging extortion tactics present risk to physical safety, such as swatting and death threats against executives.

Unique Challenges



Cyber Events Do Not Occur In a Vacuum



Partner/Vendor Communications are Often the Most Challenging



Roles & Responsibilities May Not be Clear



Incident Response is a Long Game

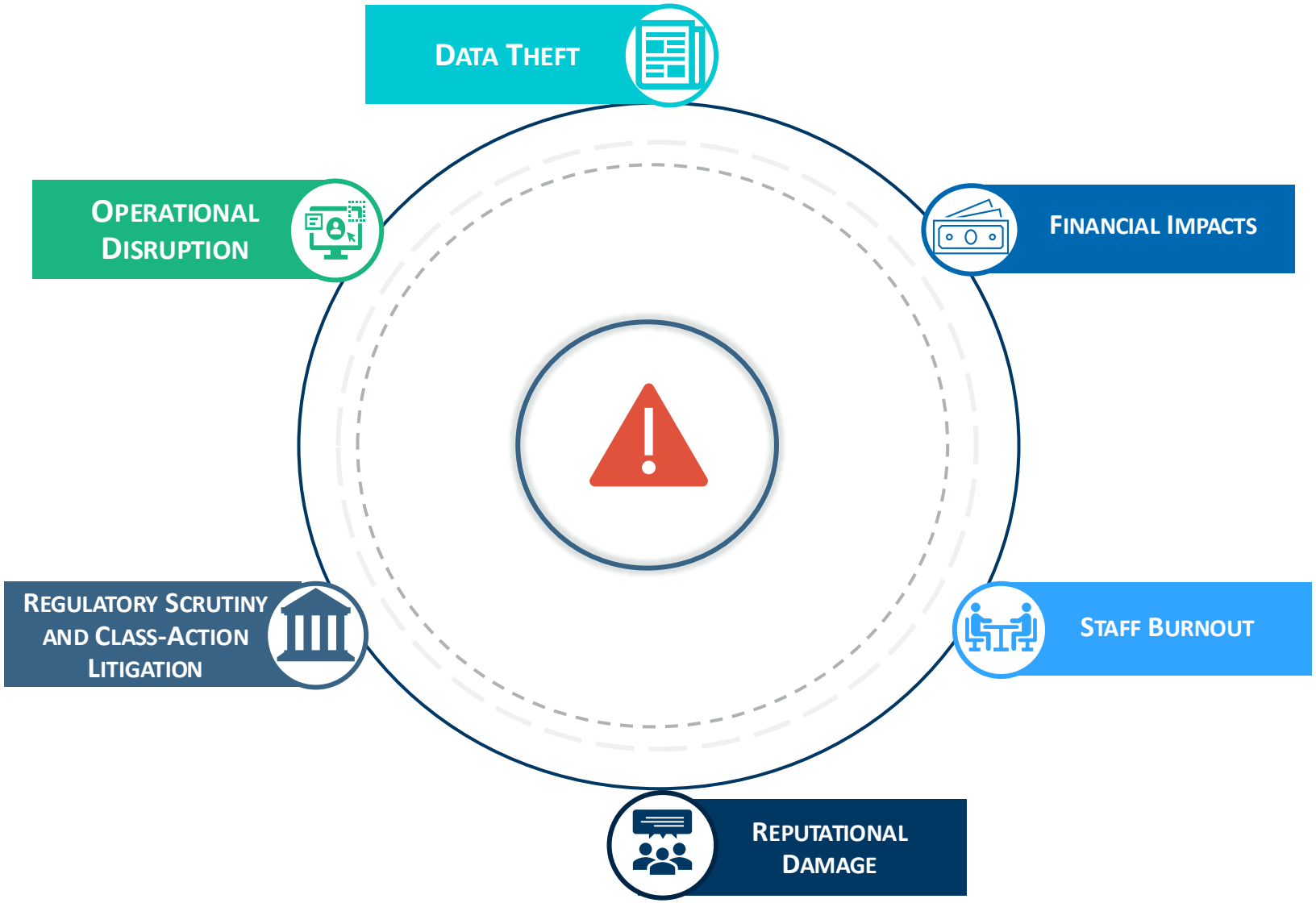


Getting Ahead of the Facts Creates Risk



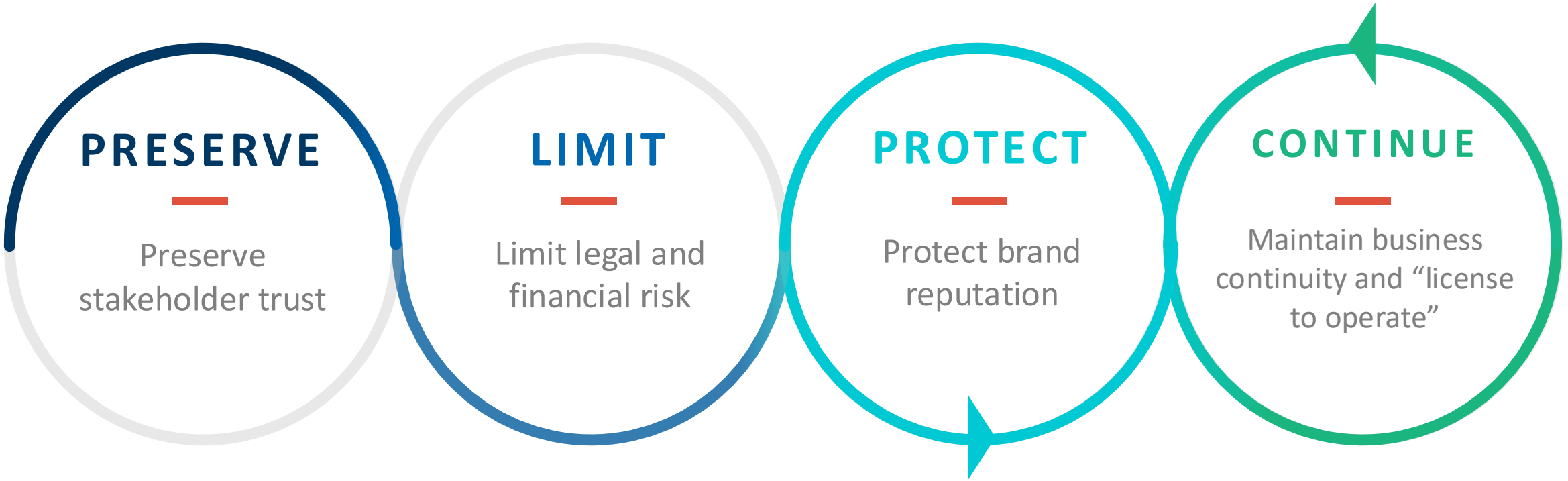
Cyber Media are Sophisticated

The Realities



Communications Best Practices

Communications Objectives



Communications Phases of Incident Response

Phase 1: Discovery of Incident, & Initial Response

(0-72 hours approx.)

Challenge: lack of confirmed information

Approach: communicate action steps

Phase 2: Containment, Remediation & Restoration

(72 hours – week 3 approx.)

Challenge: increase in stakeholder inquiries

Approach: communicate actionable information and updates

Phase 3: Forensic Investigation & Data Review

(Week 3 – onwards)

Challenge: quiet period

Approach: prepare for escalations

Phase 4: Legal Notification

(Investigation is finalized)

Challenge: legal notification requirements

Approach: pivot to reputation recovery

Breaking Down Siloes

Align Legal & Comms Strategies

Ensure legal, regulatory and communications workstreams are aligned, informed, operating under privilege

Engage Law Enforcement

Collaboration and diligence around OFAC/compliance issues are very helpful to combating stories around TA attribution

Think Holistically

Everything will be under a microscope – including, but not limited to, advertising, job postings, org structure, etc.

Identify Partners

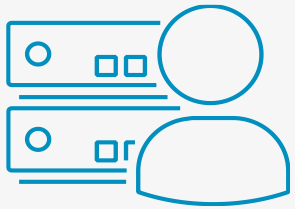
Establish relationships with key vendors and partners in advance

Communicating Effectively Amidst Fluid Facts



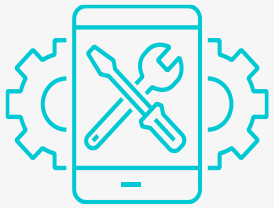
Responsiveness

Communicate actionable information to all stakeholders



Accuracy

A communications strategy is only as good as the facts on the ground; be mindful of word choice



Transparency

Convey honesty, while also balancing transparency and risk



Consistency

Consistency in message across stakeholder groups is key; "establish a single source of truth"

Focusing on Inside-Out Communications

INTERNAL COMMUNICATIONS

- Help maintain business continuity
- Minimize speculation, providing clear and consistent updates and/or directions
- Meet legal obligations to notify internal parties impacted
- Equip the front-lines for success

EXTERNAL COMMUNICATIONS

- Control public narrative surrounding the incident (once/ if made public)
- Meet legal obligations to notify impacted stakeholders
- Prepare spokesperson(s) to speak on background with reporters, if necessary

- Highlight remediation efforts, including dedication to identify the specific data stolen and safely restoring impacted systems
- Demonstrate transparency to the extent possible
- Ensure stakeholders hear about the incident from YOU first

Prioritizing Stakeholder Engagement

- 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
- Centralize inquiry management process



Cybersecurity Crisis Communications Preparedness



Define Communications Roles and Responsibility



Build Connectivity Between Key Incident Response Functions



Agree on Communications Approval Process and Communications Vehicles



Draft “hour 1” Communications Templates



Integrate Communications in Tabletops

Bringing it to life: *Scenario Run-Through*



THURSDAY
OCTOBER 22, 2026
6:45 A.M.

- A member of Nebraska Fields Hospital's Security team arrives at work and finds a ransom note displayed on their computer screen. The note advises that the hospital's computer networks have been encrypted and patient and operational data have been exfiltrated, demanding the hospital contact the threat actor to negotiate payment within 72 hours.

- As an immediate precautionary measure to contain the threat, the IT security team takes all systems offline.
  - Unavailable systems include: EHR, MyChart, email, phone system, and systems used to order certain tests, procedures, and medications.

- Patients begin receiving information that their procedures are rescheduled due to impacted services. Patients are alarmed, confused, and frightened.

THURSDAY
OCTOBER 22, 2026
6:45 A.M.

What should the organization's top communications priority be at this point?

A. Internal/Employee communications

B. Patients and families

C. Engaging with the media

D. No communications for now until more is known

THURSDAY
OCTOBER 22, 2026
2:00 P.M.

Dear Nebraska Fields Hospital Team,

I'm a reporter from the Lincoln Diamond covering health and patient safety. We have received multiple reports that your organization is currently experiencing a significant cybersecurity incident.

Several individuals have reached out to us directly, expressing concern after their surgeries were postponed or moved to other facilities without clear explanation.

Can you confirm whether a cybersecurity incident has occurred, what systems have been affected, and what steps the hospital is taking to ensure the safety and care of its patients? We are working on a deadline and would appreciate a response by 4.00 p.m. today.

Sincerely,

Chloe Hourman
Reporter, Health
The Lincoln Diamond

- Nebraska Fields Hospital activates its pre-established downtime procedures while systems remain offline.
- Individuals and families are beginning to call and reach out in large numbers after being notified that their scheduled surgeries have been postponed or delayed. Critical cases are being diverted to a nearby unaffected Nebraska facility to ensure urgent care is not interrupted.
- Local Nebraska media outlets are reaching out directly to the hospital, asking about the reported disruption and the scale of impact to patient care. The hospital has not yet told its side of the story, and without a timely response, the media will fill that gap on their own.

THURSDAY
OCTOBER 22, 2026
2:00 P.M.

How would you respond to the media inquiry?

A. Issue a brief statement

B. Decline to comment

C. Engage in a conversation on background



- The threat actor has begun reaching out directly to patients and families via calls, claiming to have information related to them to apply pressure on the hospital.
- The threat actor is demanding $50 million to provide the decryption key to restore hospital systems and suppression of the stolen patient data.
- The threat actor sets a deadline of 24 hours to respond to the demand.



What is your initial response and strategy for addressing the threat actor's direct outreach to patients?

A. Proactively contact affected patients first

B. Issue a broad public statement

C. Undecided

MONDAY
OCTOBER 26, 2026
12:45 P.M.

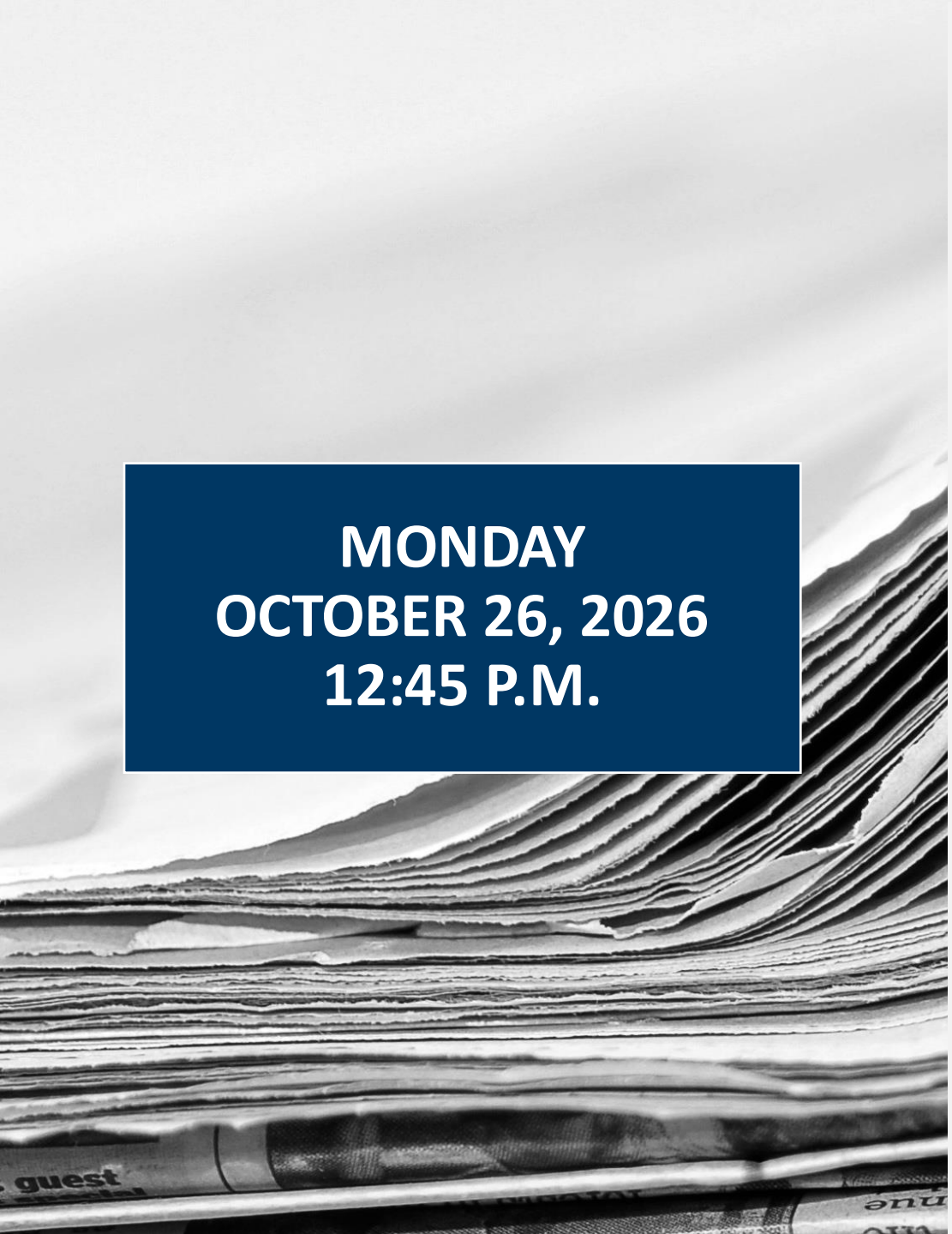


SECURITY

Patients Furious as Cyberattack Forces Nebraska Hospital to Postpone Surgeries

LAWRENCE ABRAMS Oct 19, 2026 01:33 PM 0

- Patients are growing increasingly vocal, expressing anger over disrupted services and postponed surgeries, with many taking to social media to share their frustration directly. Public pressure on hospital leadership to communicate more urgently is amplified.
- The media is reporting on the human impact of the outage, with reporters focusing on patients facing delayed procedures.
- There is progress in the restoration efforts. Email and phone services are back up and running. The team also notes that MyChart is close to being fully remediated as they continue to work to bring all systems back online.



MONDAY
OCTOBER 26, 2026
12:45 P.M.

How would you try to calm patients' concerns?

A. Send an all-family/patient letter

B. Post information on the website

C. Organize a live Q&A session



- Restoration is complete, and all systems are back up and running as normal.
- The forensic investigation confirms that patient names, date of birth, medical history, and SSNs for approximately 500,000 patients has been exfiltrated.



After the hospital completes its legal notification requirements, what's next?

A. Celebrate!

B. Go on a proactive media blitz to begin restoring reputation and trust

C. Conduct an after-action review internally

Key Takeaways

Questions to Ask Today

- ❑ Are we generally aware of risk exposure and mitigation efforts?
- ❑ Do we have relationships established with specialized cyber counsel, cyber forensics and cyber crisis communications partners?
- ❑ Do we have an updated Incident Response Plan and Crisis Communications Playbook for cyber events?
- ❑ How recent was our last cybersecurity tabletop exercise? Were senior, cross-functional leaders present?
- ❑ Is our workforce prepared for an extended downtime event?
- ❑ How would the organization communicate with key stakeholders if certain communications channels are not available?
- ❑ Who internally needs to approve a ransom payment for your organization?

Final Thoughts

1. Your Response is What Will be Remembered
2. Have a Plan and Practice
3. Don’t Go it Alone!


QUESTIONS?

99TH NHA ANNUAL
Convention

Tell us your thoughts on this session!

This quick survey takes less than a minute, and your feedback helps us improve future sessions.

SCAN HERE

NHA | NEBRASKA HOSPITALS