#NHCPC24

NATIONAL HEALTHCARE COALITION PREPAREDNESS CONFERENCE

Visions of Progress: Sustainable Strategies for Emergency Preparedness & Resilience

Presented By:

MESH

Preparing for the Operational Consequences of a Cyber Attack:

Strategies and Best Practices

Patrick Turek, Senior System Director
Public Safety and Emergency Management
Hartford HealthCare

Roger Glick, Market Director
Healthcare + Emergency Management
Jensen Hughes

“Every incident has narratives with victims, villains, and heroes.”

Eric J. McNulty
Associate Director
National Preparedness Leadership Initiative
Harvard University

Learning Objectives

01

Understand the potential impact of cyber attacks on healthcare operations.

02

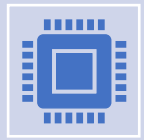
Describe key elements of an effective preparedness strategy.

03

Enhance an organization's preparedness for the operational consequences of a cyber attack.

Discussion Points

How likely is it that your organization will experience a cyber attack in the next five (5) years?

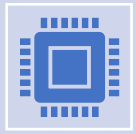


How disruptive would a cyber attack be to your normal operations?

#NHCPC24

Discussion Points

How likely will your organization experience a cyber attack in the next five (5) years?



How disruptive would a cyber attack be to your normal operations?

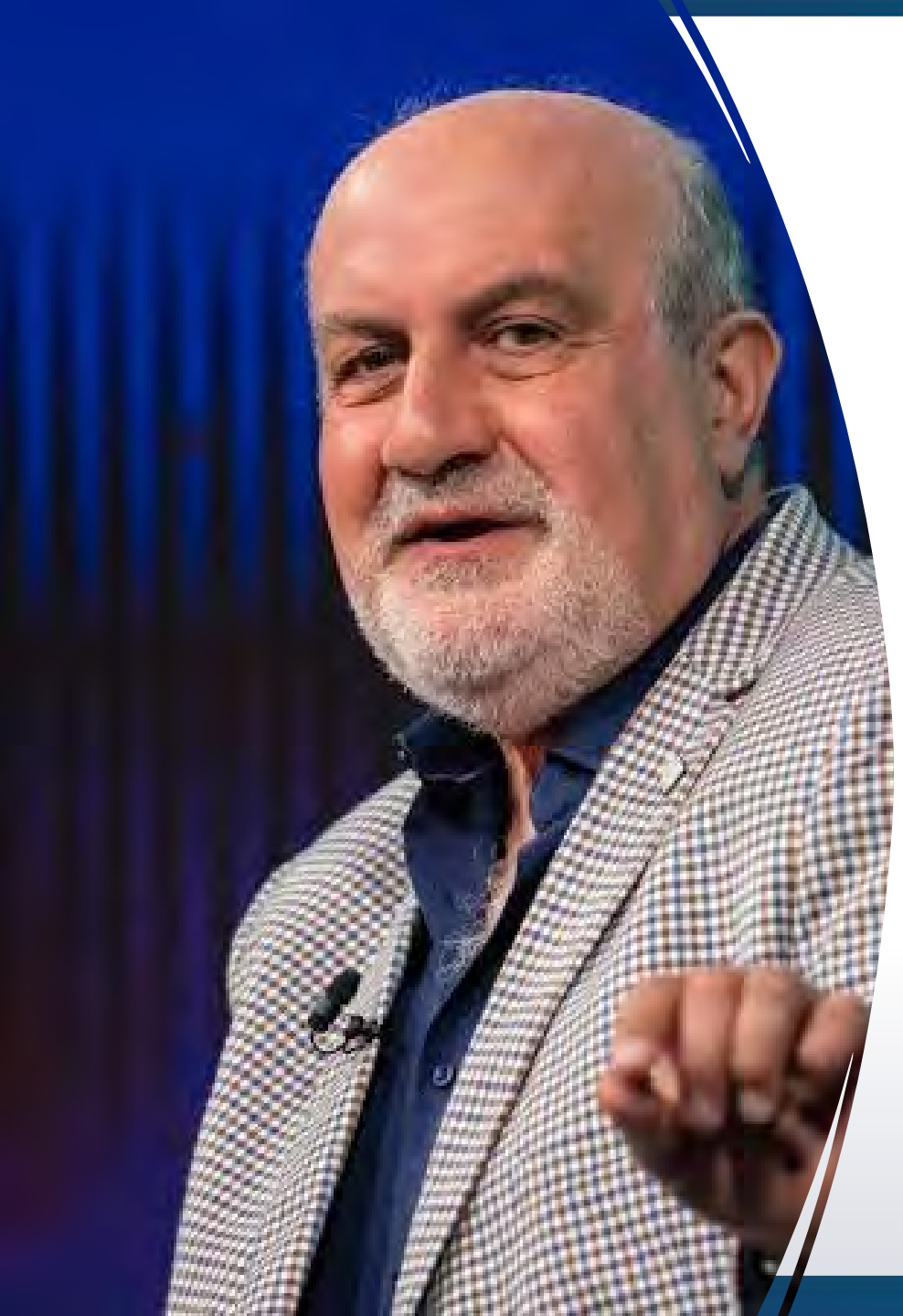
What has your organization done to prepare for a cyber attack?

Discussion Points

- How likely will your organization experience a cyber attack in the next five (5) years?
- How disruptive would a cyber attack be to your normal operations?
- What has your organization done to prepare for a cyber attack?
- Has the risk of your organization being hit by a cyber attack changed?

Discussion Point

- How likely will your organization experience a cyber attack in the next five (5) years?
- How disruptive would a cyber attack be to your normal operations?
- What has your organization done to prepare for a cyber attack?
- Has the risk of your organization being hit by a cyber attack changed?
- How has your organization’s preparedness changed to reflect that increased risk?



We underestimate risk: we believe negative events are less likely to happen to us (Optimism Bias).

We overestimate preparedness: we believe we are prepared for crises and that the risks are fully manageable when, in reality, their complexity often exceeds our abilities (Illusion of Control).

Nassim Nicholas Taleb

The Black Swan

So, what is an effective preparedness strategy?

A Preparedness Strategy

Risk Reduction is primarily an IT function. Although EM/BC should be an active participant, it is NOT the "lead" – for obvious reasons. IT identifies and coordinates strategies to decrease the risk of cyberattacks (e.g., implementing Multi-Factor Authentication, keeping IT systems updated and patched, Employee Awareness, and Training Programs).

A Preparedness Strategy

<u>Consequence Management is primarily an EM/BC function.</u>
Developing strategies and plans, training key stakeholders on those plans, and exercising the plans to evaluate them are all responsibilities of EM/BC.

A Preparedness Strategy

Develop Consequence Management Strategies and Plans:

- Map out the organization as a system.
- Identify potential disruptors to the system.
- Ask “what ifs”. Boldly explore worst-case, not best, scenarios.

Use this information to inform Scenario-based Planning.

A Preparedness Strategy

Consequence Management Strategies and Plans

Develop a Cyber Attack Playbook for Incident/Organization Leaders

- Immediate Actions Checklist
- Description of Crisis Response Phases and Roles/Responsibilities/Authority
- Legal Workflows and Timing (e.g., Hiring a Negotiator, Engaging the Threat Actor, Engaging Law Enforcement, Reporting and Notification Obligations)
- Ransom Payment Guidelines

A Preparedness Strategy

Consequence Management Strategies and Plans

- Strategies
  - Ensure patient safety
  - Minimize disruption to normal operations
  - Protect patient, employee, and organization information
  - Protect the organization's reputation
  - Recovery priorities (e.g., software/function, organizational geography)
- Plans
  - Clinical management plans (e.g., EMR, imaging, pharmacy, case management)
  - Staffing management plans (e.g., scheduling, payroll, employee assignments)
  - Facility management plans (e.g., security/access, HVAC systems, alarm monitoring systems)
  - Financial management plans (e.g., accounts receivable, accounts payable, pre-authorizations)

A Preparedness Strategy

Training and Exercising

- Training is essential
  - Different people will need to be trained on different plans.
  - Different people will need different levels of sophistication and competence.
  - Training programs must be developed to combat knowledge decay and staff turnover.
- Exercising is also essential
  - The purpose of an exercise is to evaluate the plan (and, to a lesser extent, the responders).
  - The exercise program should have increasing complexity (e.g., severity, duration, and co-morbidities).
  - The exercise program should stress-test the system (e.g., stress till failure and then build back stronger).
  - The exercise program should always identify opportunities that are then leveraged improvements.

Case Study: Hartford HealthCare

Hartford HealthCare is one of Connecticut's most comprehensive health care networks.

Fast Facts:

- President & CEO: Jeffrey Flaks
- Licensed Beds: 2,488
- Colleagues (incl. employees and contingent staff): 27,701
- Physicians on Staff: 5,847
- Operating Revenue: $5,403,735,000

“While an initial crisis may not have been preventable, the secondary crisis of a bungled response is avoidable.”

Eric J. McNulty
Associate Director
National Preparedness Leadership Initiative
Harvard University

Questions

Speakers

Patrick Turek, Senior System Director
Public Safety and Emergency Management
Hartford HealthCare
patrick.turek@hhchealth.org

Roger Glick, Market Director
Healthcare + Emergency Management
Jensen Hughes
roger.glick@jensenhughes.com
540.521.7996