A Framework to Support Healthcare Continuity of Operations in an Information Technology Failure:

*Lessons learned from a novel exercise series*

Jendy Dunlop, MPH, CHEP

Paul Biddinger, MD, FACEP

PERRC

HARVARD SCHOOL OF PUBLIC HEALTH
Emergency Preparedness and Response Exercise Program
Workshop Objectives

Following today’s presentation, participants will learn:

• Why and how the healthcare system is uniquely vulnerable to information technology (IT) disruptions and the operational consequences of unplanned downtimes;

• How to apply lessons learned from the exercise series to guide and maximize collaborative preparedness efforts between emergency management and information technology personnel; and

• How to utilize a planning framework to develop and guide continuity of operations planning for IT system failures and unplanned downtimes at their own institutions.
Introduction

Harvard School of Public Health Emergency Preparedness and Response Exercise Program (HSPH-EPREP)

Mission:

To provide public, private, and non-governmental organizations with the expertise to prepare for and respond to emergencies of all types.
Since exercise program inception in 2005, we have conducted over 50 public health and healthcare exercises throughout Massachusetts.

**HSPH-EPREP Exercises and Participation 2005-Present**

<table>
<thead>
<tr>
<th></th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exercises</td>
<td>4</td>
<td>14</td>
<td>8</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>10</td>
<td>8</td>
<td>24</td>
<td>2</td>
<td>94</td>
</tr>
<tr>
<td>Participants</td>
<td>522</td>
<td>2,318</td>
<td>1,361</td>
<td>666</td>
<td>951</td>
<td>808</td>
<td>762</td>
<td>546</td>
<td>885</td>
<td>225</td>
<td>9,044</td>
</tr>
</tbody>
</table>
Massachusetts Department of Public Health & Harvard School of Public Health Statewide Exercises:
Capabilities Demonstrated and Assessed
2006 - 2014

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pan-Flu 2006</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COOP 2006</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hospital Evacuation TTX Series 2010</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medical Surge TTX Series 2011</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HazMat TTX Series 2011-2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regional Coalition Series 2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medical Surge FE Series 2012-2013</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery Workshop Series 2013</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETCFC Exercise Series 2013</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Healthcare System Recovery Series 2013</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mass Fatality/FAC Exercise 2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Background

February 2009: **Health Information Technology for Economic and Clinical Healthcare Act** (HITECH) enacted as part of the American Recovery and Reinvestment Act.

- Federal investment in health information technology (HIT)
- Mandates public and private healthcare providers to adopt electronic health records (EHR)
- Incentives to providers demonstrating ‘meaningful use’ of systems
Background

Since 2009, adoption of EHR systems by U.S. hospitals has more than tripled.

**Figure 1:** Percent of non-federal acute care hospitals with adoption of at least a Basic EHR system and possession of a certified EHR: 2008-2012
(ONC, No. 9, March 2013)

**Figure 1:** Percent of non-federal acute care hospitals with adoption of EHR by levels of functionality (ONC, No. 9, March 2013)
Background

Figure 3: Percent of non-federal acute care hospitals with computerized capabilities to meet selected Meaningful Use objectives: 2008-2012
(ONC, No. 10, March 2013)

Figure 4: Percent of non-federal acute care hospitals with capability to meet Meaningful Use objectives: 2011-2012
(ONC, No. 10, March 2013)
Electronic systems are used to manage virtually all aspects of daily operations at many hospitals and healthcare facilities:

- **Patient Care**
  - Medical Records
  - Imaging
  - Prescriptions
  - Labs

- **Facilities Management**
  - HVAC
  - Security systems
  - Access cards
  - Infant abduction systems

- **Administration**
  - Billing
  - Payroll
  - Communication systems
Background

2013 Meritalk/EMC\textsuperscript{2} survey finds that security breaches, data loss, and unplanned system outages cost U.S. healthcare providers more than $1.6 billion per year.

In the last year, healthcare organizations have experienced the following:

- **Security Breach**: 19% have experienced. Causes include:
  - 58% Malware/viruses
  - 42% Outsider attacks
  - 38% Physical security

- **Data Loss**: 28% have experienced. Causes include:
  - 51% Hardware failures
  - 49% Loss of power
  - 27% Loss of backup power

- **Unplanned Outage**: 40% have experienced. Causes include:
  - 65% Hardware failures
  - 49% Loss of power
  - 31% Software failures

Meritalk/EMC \textsuperscript{2}Global IT Trust Curve Study, (2013).
Figure 1: Common Causes of Unplanned Outages in Healthcare Information Technology Systems

- Hardware failure (65%)
- Loss of power (49%)
- Software failure (31%)
- Data corruption (24%)
Background

Unplanned Outages

- 40% of healthcare organizations have experienced within past year
- Average of 57 hours lost to downtime
- Consequences of unplanned downtime translate to a 45% reduction in employee productivity
- Average cost of $432,000 per incident
- Average cost of over $515 million to U.S. hospitals
December, 2011: Gwinnett Medical Center, Atlanta, GA

- Malware breach led to 3 day outage; Hospital forced to go on total diversion for over 2 days
- Disrupted connectivity at 2 hospital campuses
- Delays to patient registration, labs, radiology, pharmacy
- Implemented downtime procedures and used runners
- Cause unknown, but believed to be from corrupted thumb drive or use of personal laptop on hospital’s network
March, 2013: Boulder Community Hospital, Boulder, CO

- Primary and backup server malfunctions caused Meditech system crash and resulted in **10 day outage**
- Main hospital campus, satellite campus, 8 labs and 6 imaging centers unable to access patient information
- Experienced challenges with implementation and use of paper-based methods
- Caused significant delays in patient scheduling, diagnostic imaging, labs
- Loss of data from EHR system; even recently backed up data was corrupted
Background

- With rapid adoption of ever-evolving technology, the healthcare sector is becoming increasingly dependent on information technology as a **mission critical resource** in support of routine clinical and business operations.

- As this dependency increases, so does the level of **vulnerability** to system breaches, system failures and unplanned downtimes.
Open Discussion

- Has your facility experienced any unplanned IT outages in the past year?
  - What was the approximate duration of the outage?
  - What was the cause?
  - How did this incident impact your facility?
Exercise Series

• In 2011, a consortium of Boston-area hospitals recognized the threat that such disruptions pose to health system continuity of operations, and in turn, to patient safety.

• Between 2011 and 2013, HSPH-EPREP was contracted to design and conduct exercises for various Massachusetts hospital systems in order to assess healthcare system operations in light of IT disruptions.

• Exercised with both robust hospital systems, as well as smaller hospital systems with in-house resources.
Exercise Overview

Exercise Design: Tabletop and Functional Exercise

- Simulated system-wide information technology failure impacting patient care
- Designed to test individual and collective site response

Exercise Play:

- Simultaneous exercise play across all hospital system sites including acute care hospitals, rehabilitation facilities, home healthcare agencies, and satellite offices
- Emergency Management and Information Technology Lead Player at each site
- Participation from departments including, but not limited to: Nursing, EDs, ORs, Labs, Radiology, Scheduling, Transport, Dietary/Food Service, Finance, and Information Technology
Exercise Overview

Exercise Evaluation:

• Trained Controller/Evaluator at each site
• Formal hotwash following exercise play
• After Action Report and Improvement Plan (AAR-IP) documenting key findings, and recommendations to address areas for improvement
## Capabilities Tested

**Table 1. Healthcare Preparedness Capabilities Relevant to Exercise**

- Healthcare Preparedness Capability 3: Emergency Operations Coordination
- Healthcare Preparedness Capability 6: Information Sharing

**Table 2. FEMA/DHS Target Capabilities Relevant to Exercise**

- Target Capability 1: Planning
- Target Capability 2: Recovery
- Target Capability 3: Communications
- Target Capability 4: Intelligence and Information Sharing and Dissemination
Exercise Objectives

1. Test **internal and external notification processes** within and among sites following a major IT system failure.

2. Examine the process by which sites **assess the scope of impact** of the event and maintain situational awareness.

3. Determine the **strengths and weaknesses** of existing **downtime manual processes**.

4. Evaluate the procedures for **prioritizing restoration** of IT systems within and among sites.

5. Evaluate the level of **recovery planning**/ability to return to normal operations.
Exercise Scenario Snapshot

A malware virus has infiltrated the hospital system servers by way of medical devices operating on outdated versions of Microsoft Windows. The widespread infection results in significant degradation to computer systems, applications, and machines, along with a secondary loss of communications capability including internet, email, and phone lines across sites. The incident occurs at the height of flu season, with most hospital Emergency Departments at or near capacity.
What would your facility do?
Common Challenges

EOC & Information Sharing

- Incident management & leadership: Who is in charge?
- Communication between clinical, emergency management, and IT personnel, and across multiple sites

Healthcare Preparedness

- Difference between routine outages & outages potentially requiring an emergency response
- Anticipating when to transition to downtime procedures
- Knowledge of other departments’ and sites downtime procedures
- Realization that downtime procedures would not adequately address needs in an extended outage.
- Knowledge regarding interconnectedness of systems

Healthcare Recovery

- Leadership & decision making regarding a process for bringing systems back online within and across sites
- Awareness of clinical and operational needs, and staff roles and responsibilities in recovery
- Knowledge of HIPPA and other regulations concerning patient confidentiality issues, data loss, reporting, and insurance reimbursement timeframes
Key Lessons Learned
Key Lessons Learned

During outages necessitating an emergency response, IT leadership personnel should be incorporated within the existing hospital Incident Command structure.

Pre-defined, tested, redundant alerting mechanisms and communication protocols should be developed to promote situational awareness with IT personnel as well as with other sites.
Key Lessons Learned

Healthcare Preparedness

• Unplanned outages/system downtimes should be viewed as a **potential emergency event** requiring an emergency response. Pre-define triggers and protocol that should be followed to assist staff in recognizing emergent vs. non-emergent outages.

• When possible, a decision to transition to downtime procedures should be centralized and coordinated across units/departments and/or sites. Pre-define triggers and protocol to alert staff when and how these transitions will occur.
Key Lessons Learned

Healthcare Preparedness

• A thorough risk assessment of systems, system vulnerabilities and interdependencies, and clinical impacts associated with system failures should be conducted in advance of an incident.

• Traditional downtime processes are often designed for outages of shorter duration (hours, days) and will likely fail to adequately address operational needs during outages of extended duration (multiple days/weeks). Ensure downtime procedures are scalable to address clinical and operational needs in short term and long term outages.
Key Lessons Learned

Healthcare Recovery

• A mechanism to categorize systems and applications within a hierarchical structure, and to prioritize them for repair should be developed in advance of an incident.

• Recovery planning should begin early on in the response phase, and operate in tandem with response efforts.

  • *Best practice: Appointing a branch within the Planning Section to recovery needs/considerations*
Preparedness Framework for IT Failures

Emergency Management ➔ Information Technology

ASSESSMENT

EVALUATION ➔ PLANNING

HARVARD SCHOOL OF PUBLIC HEALTH
Emergency Preparedness and Response Exercise Program
Assessment

Hazard Vulnerability Analysis (HVA) required annually for hospitals by Joint Commission in order to “identify potential emergencies that could affect the hospital’s demand for services or its ability to provide those services, the likelihood of those events occurring, and the consequences of those events”. (EM 01.01.01)

- No specific tool or resource required to complete

- “All hazards” risks; nowhere near specific enough to assess the intricacies of IT systems, the likelihood of and associated impacts of IT failures

- Most organizations have not recognized the true potential for an internal information systems failure to constitute a true emergency
Conduct an independent, comprehensive assessment of IT systems, system vulnerabilities, system interdependencies, and clinical and operational consequences of system failures. At a minimum, the assessment should determine the following for each electronic system/process:

- Interdependent, connected systems;
- Anticipated clinical and operational impacts associated with system/process loss;
- Whether downtime/paper procedures exist to address the electronic process;
- Whether downtime procedures to address the electronic process adequately meet needs in an extended outage;
- Whether all appropriate staff have been trained to utilize downtime procedures addressing the electronic process; and
- Extent to which downtime procedures are drilled/tested with staff during all shifts.
## Assessment

- Determine if existing downtime procedures are scalable to appropriately address both short term and long term operational needs.

- Review the adequacy of downtime training, drills, and exercises for staff.

- Review incident recognition, alert and notification, response, and recovery procedures between emergency management and IT personnel for a system downtime event.

- List all anticipated clinical, operational, and financial recovery needs and considerations.
## Planning

- Develop and/or revise alert and notification, communication, and information sharing plans and processes between emergency management and IT personnel in response to a systems failure. Ensure specific triggers exist to indicate when notifications and key decisions should be made.

- Develop and/or revise plans to address identified gaps in emergency management and IT systems, policies, and procedures.
<table>
<thead>
<tr>
<th>Planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Based on your assessment of systems, develop a scalable tiered or phased plan for prioritizing specific systems for repair within and across sites.</td>
</tr>
<tr>
<td>- Train staff on all shifts to increase comfort and familiarity in using downtime procedures.</td>
</tr>
<tr>
<td>- Update plans to include long term recovery considerations.</td>
</tr>
</tbody>
</table>
## Evaluation

- Design and conduct periodic drills and exercises through the lens of emergency management plans and procedures. Focus on emergency management and IT response system linkages.

- Conduct a hotwash to review exercise results, identify remaining gaps in plans and procedures, and determine appropriate solutions. Document successes and lessons learned in an After Action Report and Improvement Plan (AAR-IP).
Open Discussion

• Has your facility developed any specific plans or protocols as a result of any unplanned downtimes experienced?

• What do you see as the biggest barrier to facility preparedness for a large scale information technology failure?

• What would be most beneficial to you to assist you with future planning for preventing, preparing for and responding to IT system outages?
-Thank You-

Thank you for your attendance and participation.

We are happy to answer any questions you may have.

Jendy Dunlop, MPH, CHEP
Project Coordinator
jdunlop@hsph.harvard.edu

Paul Biddinger, MD, FACEP
Program Director
pbiddinger@hsph.harvard.edu

http://www.hsph.harvard.edu/eprep