Information Technology Incident Management

Charles S Sawyer, MD, FACP
Justin Meadows
Jay Capodiferro

Disclosures

All of the presenters are full time employees of Mission Health System and have no conflicts of interest to disclose.

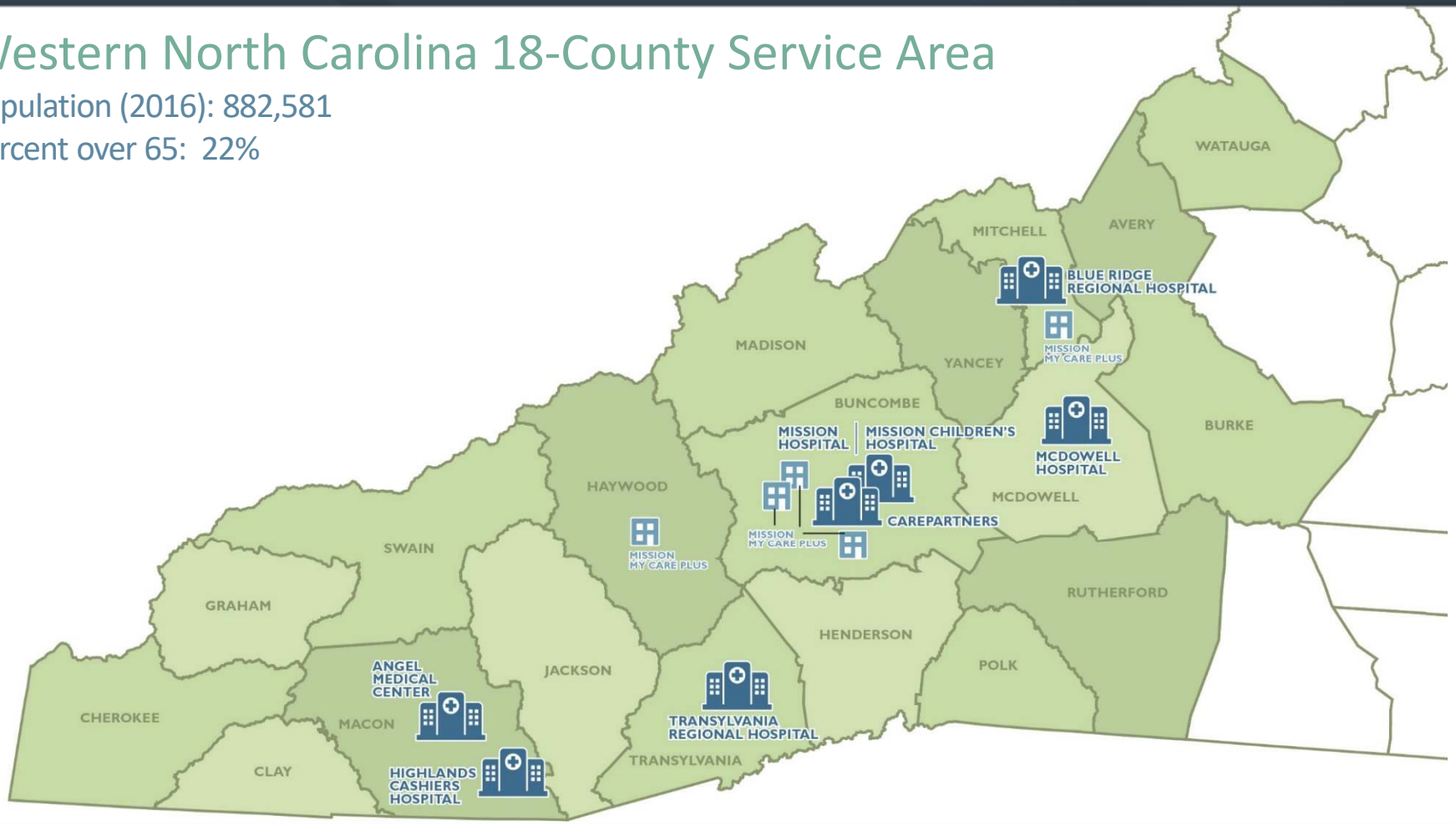

Our BIG(GER) Aim:
To get every person to their desired outcome, first without harm, also without waste and always with an exceptional experience for each person, family and team member.

MAP OF MISSION HEALTH SYSTEM

Western North Carolina 18-County Service Area

Population (2016): 882,581

Percent over 65: 22%



MISSION HEALTH

Mission Health System

- 6th largest health system in North Carolina and the only tertiary care regional referral center in Western North Carolina.
- Region's only Level II Trauma Center
- 17th largest employer in North Carolina
  - Accounting for 1 in every 16 jobs in Buncombe and Madison Counties
  - 1 in every 39 jobs in the 18 county service region
- Creates more than $1.04B economic activity in Buncombe and Madison counties and nearly $2B across the region

MISSION BY THE NUMBERS*

Total Patient Days	235,490
Total Discharges	48,027
Average LOS	4.9
Average Daily Census	645
Case Mix Index	1.6993
Total Surgery Cases	46,421
Total ED Visits	169,648
Total OP Visits	475,158
Total MAMA Flights	1,035
Total Physician Visits (employed)	537,354

*FY 16 as of 7/1/16

MISSION HEALTH


HealthCare's
most wired
WINNER 2016


BEST
HOSPITALS
U.S.News
& WORLD REPORT


TRUVEN HEALTH ANALYTICS
15 TOP
HEALTH SYSTEMS
2015


TRUVEN HEALTH ANALYTICS
15 TOP
HEALTH SYSTEMS
2014


TRUVEN HEALTH ANALYTICS
15 TOP
HEALTH SYSTEMS
2013


Modern Healthcare
Modern Physician
50 Most Influential
Physician Executives
In Healthcare


MISSION
HEALTH
Truven Health Analytics | IBM Watson Health
15 TOP
HEALTH SYSTEMS
2017


THOMSON REUTERS
15 TOP
HEALTH SYSTEMS
2012

Incident Management BEFORE

- Documented in SharePoint (if at all)
- No cross-reference to ticketing/incoming support calls
- Management/leadership managed by rotating technical and application managers (7 resources).
- No categorization, reporting or post-incident follow-up
- RCA left up to manager or owning group
- Poor change management contributing to self-inflicted incidents and concurrent incidents.
- Poor internal and external communication regarding recognition, updates and closure of incidents.
- Senior IT leadership often “informed” of incidents by other health system leadership before IT even aware

Recognition of Need

- A standardized approach to incident management
- Standardization of:
  - Definitions and roles
  - Evaluation of incidents
  - Communication
  - Documentation
  - Root cause analysis
  - Prevention of recurrences
  - Identification of Trends

Hospital Incident Command System

- A flexible, scalable, and adaptable system
- That can be used by all hospitals regardless of size, location, patient acuity, patient volume, or hazard type.
- HICS expands or contracts relative to the needs of the situation.
- By using HICS, hospitals adopt a nationally recognized system that promotes successful incident management

http://hicscenter.org/Shared%20Documents/HICS_Guidebook_2014_7.pdf

Hospital Incident Command System

- Assigns positions only as determined by the scope and magnitude of the incident
- In keeping with the principle of scalability, which is important during an emergency.
- Staff assigned positions are returned to their normal work functions once their position is no longer needed for the incident response

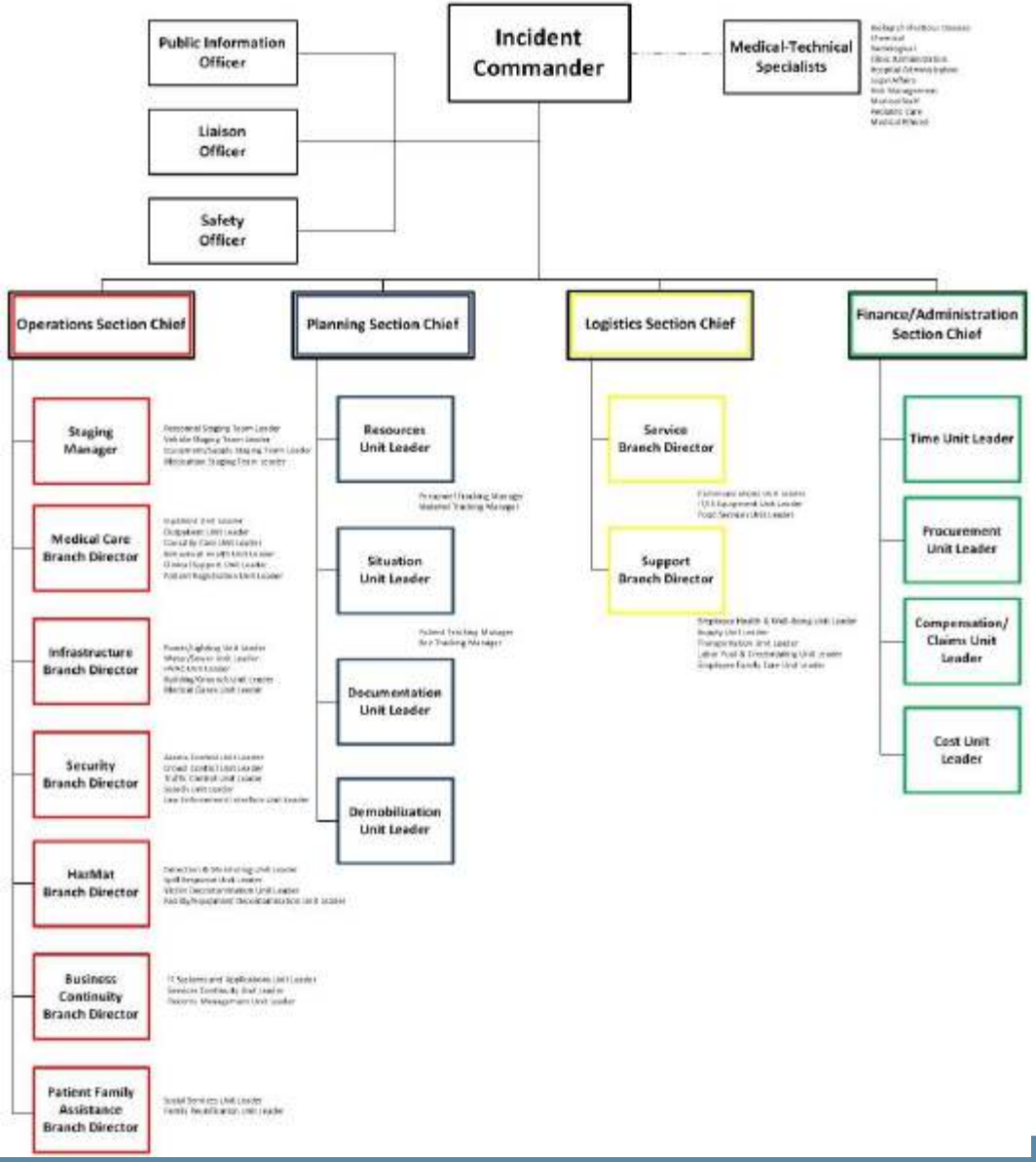
http://hicscenter.org/Shared%20Documents/HICS_Guidebook_2014_7.pdf

Foundational Principles

- Predictable chain of command with a suggested span of control
- Accountability of position and team function, including prioritized action checklists
- Common language for promoting communication
- A flexible and scalable incident management system addressing planning and response needs of any size hospital with universal applicability
- Modular design and adaptability allowing planning and management of non-emergent incidents or events
- Management by Objectives (MBO) in which the problem encountered is evaluated, a plan to remedy the problem identified and implemented, and the necessary resources assigned

http://hicscenter.org/Shared%20Documents/HICS_Guidebook_2014_7.pdf

Hospital Incident Management Team



MISSION HEALTH

Could Hospital Incident Command serve as a framework for IT Incident Management?

HICS + ITIL + ITSM

- Hospital Incident Command System
  = framework understood by our clinical and business areas

- Information Technology Infrastructure Library (ITIL) and Information Technology Service Management (ITSM)
  = framework well understood by IT industry

We then formed a small team that worked together to create a Major Incident and SPRNT process that combined what we believe are the best of both frameworks!

Major Incident Process

- This process aligns most closely with ITIL and ITSM.
- Integrates into our existing Incident Management process for everyday incidents.

- **Incident:** an unplanned interruption to an IT service or reduction in the quality, including reliability and availability, of an IT service or any component part of that service.
- **Major Incident:** an event which has significant impact or urgency, which demands a response beyond the routine Incident Management process.

Major Incident Process

- Major Incident further defined…
  a) May either cause, or have potential to cause, impact on business critical services or systems;
  b) Or be an incident that has significant impact to patient care or Mission Health System revenue;
  c) Or be an incident that has significant impact on reputation, legal compliance, regulation or security of the organization.

Problem Management Process

- This process “catches” Major Incidents after restoration of service.
- In Problem Management we focus on…
  a) Documenting the recurrence of incidents by associating them with a Problem.
  b) Documenting “workarounds” until a complete resolution can be implemented to prevent the incident in the future.
  c) Performing and documenting root cause analysis for each incident.
  d) Ensuring incidents do not keep recurring or that impact is minimized.

Incident and Problem Manager Role

- Created a full-time position to manage day-to-day activities for Incident and Problem Management.
- This created a single point of contact for incident escalation.
- While also providing consistent and standardized management of the processes instead of rotating responsibility through existing managers.
- It also gave us the resources we needed to report out on and understand more about our incidents (which we'll cover later).

Major Incident Process

- Major Incident further defined…
  - In order to operationalize the Major Incident qualification in our ticketing system, we provided criteria to guide the consistent designation of **Impact** and **Urgency** used by the Incident Manager.

Impact Criteria:

High	If ANY of these apply: • Impacted critical service that affects one or more hospitals or physician practices. • Negative impact on patient care, patient documentation and/or patient/employee safety. • Impact to 100 or more users.
Medium	Unavailability of a service that affects a single hospital, physician practice or a group of 50 to 100 users.
Low	Unavailability of a service that affects 1 user or degradation of a service impacting less than 50 users.

Major Incident Process

- Major Incident further defined…
  - In order to operationalize the Major Incident qualification in our ticketing system, we provided criteria to guide the consistent designation of **Impact** and **Urgency** used by the Incident Manager.

Urgency Criteria:

High	If ANY of these apply: • Impacted critical service that *will* lead to legal or financial repercussions. • Negative impact on patient care, patient documentation and/or patient/employee safety.
Medium	Impacted service is important to the business and *could* lead to legal or financial repercussions.
Low	Impacted service is valuable to the business, but the business can operate normally via an alternative or manual procedure.

Major Incident Process

- Major Incident further defined…
  - In order to operationalize the Major Incident qualification in our ticketing system, we provided criteria to guide the consistent designation of **Impact** and **Urgency** used by the Incident Manager.

The result determines the Severity.

Impact \ Urgency	High	Medium	Low
High	SEV 1	SEV 2	SEV 3
Medium	SEV 2	SEV 2	SEV 3
Low	SEV 3	SEV 3	SEV 4

SPRNT

Service and
Performance
Restoration and
Normalization
Team

- This process aligns most closely with the HICS system.
- In some incidents, a formalized response effort is required to mitigate impact, manage risk, communicate to the organization and implement fixes and workarounds.
- Colloquially this was referred to as an **IT Command Center**.
- This conflicted with our **Hospital Incident Command** nomenclature.

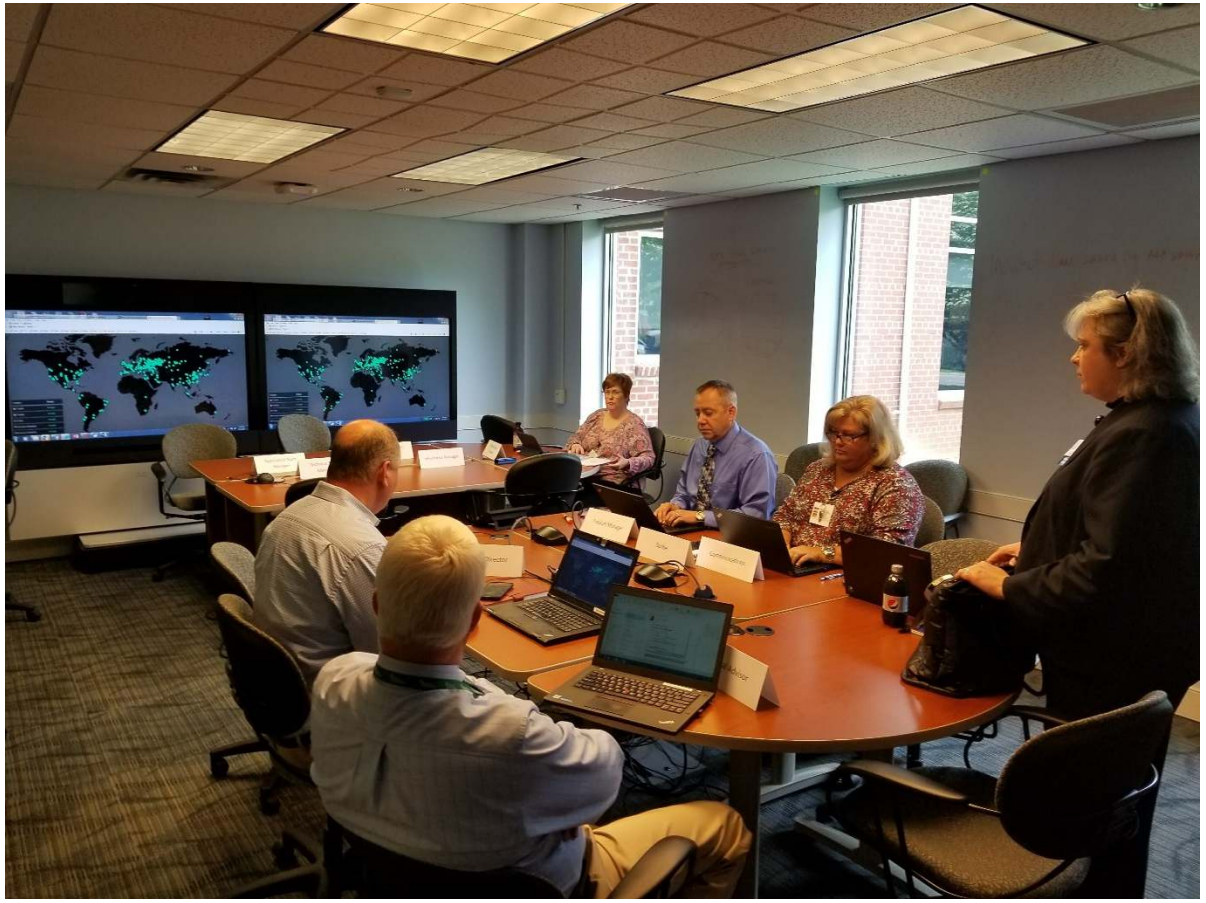
SPRNT modeled after HICS

- While we changed our name, we borrowed heavily from HICS to structure our response team and enable it to “snap-in” to the HICS system when the Hospital Command Center was activated.
- A SPRNT is initiated for **Severity 1** incidents at the discretion of the Incident Director upon escalation from the Incident Manager.
- 6 of our critical services require an automatic SPRNT if they cannot be resolved in 45 minutes.

SPRNT Roles

- Similar to HICS, the SPRNT team has designated roles with documented responsibilities to be performed by each role.
  - Incident Director
  - Application Team Manager
    - Application Team Member
  - Informatics Manager
    - Rounder
  - Medical Advisor
  - Technical Team Manager
    - Architect
    - Technical Team Member
  - Problem Manager
  - Communications
  - Logistics
  - Scribe

SPRNT Response to WannaCry



SPRNT Response to WannaCry

MISSION HEALTH

SPRNT Briefings

- SPRNT briefings are formalized.
  - Usually top of the hour, depending on timing of the incident.
  - Report outs/updates communicated 15 minutes prior to the briefing.
  - Incident Director reviews current status and documents any planned actions.
  - Emergency Change Management procedures are overseen by the Incident Director.

SPRNT Communications

- A formal communication process is executed.
  - Initial briefing
  - **Initial status communication (internal to IT)**
  - Initial status communication (external to IT)
  - Notification to House Supervisor
  - App and Technical Status (:45 on the hour)
  - Briefing (top of every hour)
  - **Ongoing internal and external status communications**
  - Final briefing on resolution
- Most internal communications are facilitated through an integration of our ITSM system with **Everbridge**.

SPRNT + HICS Snap-In

- In the event that the Hospital Command Center (HCC) is activated…
  - SPRNT team becomes a sub-cell
  - IT representative physically or remotely joins their team
  - All external to IT communications are managed by the HCC
    - Distribution many times is managed by SPRNT in coordination with the HCC
    - Internal IT communications continue uninterrupted

- Our designated SPRNT conference room also serves as the backup Hospital Command Center.
  - Equipped with staged-and-ready radio, telecom and wireless equipment as well as printed materials to support the HCC team.

SPRNT After Action Review and MOCK

- For each SPRNT we follow-up with an After Action Review (AAR) to review what went well and what can be improved.
- We also schedule MOCK incidents quarterly to practice our response efforts and keep everyone fresh in the absence of major incidents to manage.

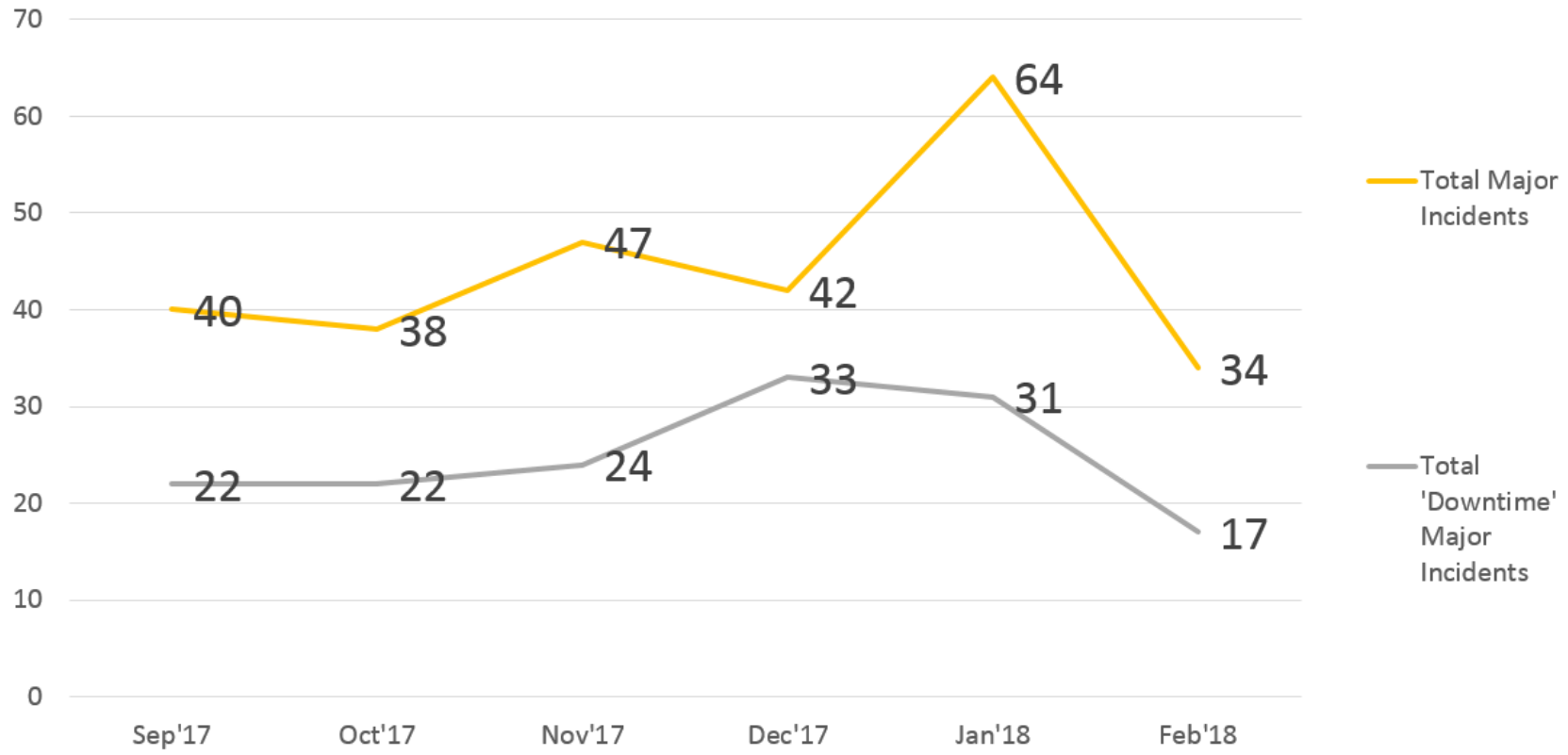
What did the data tell us about all of this process that was implemented?

MISSION HEALTH

Key Metric Focus Areas

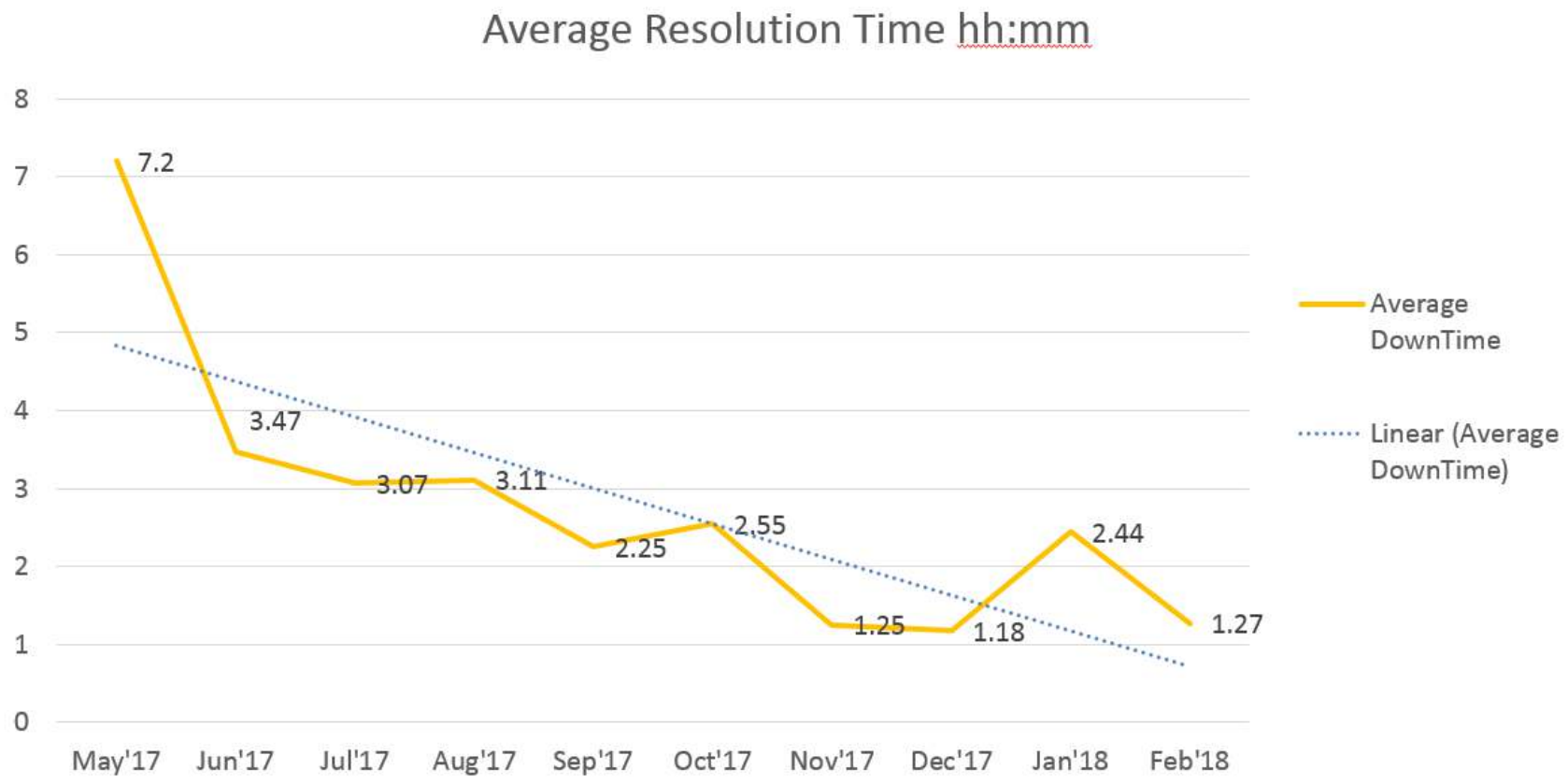
- Downtime versus Non-Downtime Incidents
  - Internally Responsible
  - Vendor Responsible
  - Caused by Change
- Time to Resolution
  - Internal Response Time (Process)
  - Vendor Response Time (Escalation)
- Root Cause Analysis
  - What are you going to do with it?

Statistical Results



MISSION HEALTH

Resolution Time Improvement



MISSION HEALTH

Process Improvements

- Monitoring/Event Management
  - Proactive Incident/Problem Management
- Escalation
  - Who's on-call?
  - Vendor escalation paths.
- Communications
  - Content
  - Schedule

Thank you

Questions?

MISSION HEALTH