Surviving a Cyber Attack: An Operational Perspective

March 5th, 2018

Sara Gibbons, MSN, RN-BC, CPN, Sr. Director & CNIO
Daniel Nigrin, MD, MS, SVP Information Services & CIO
Laura Wood, DNP, MS, RN, NEA-BC, SVP Patient Care Operations & CNO

Boston Children's Hospital
Until every child is well™

Conflict of Interest

Sara Gibbons, MSN, RN-BC, CPN
Daniel Nigrin, MD, MS
Laura Wood, DNP, MS, RN, NEA-BC

Have no real or apparent conflicts of interest to report.

Agenda

- The Hacktivist Attack
- Lessons Learned/Prevention
- Parallels to EHR Downtime/Operational Impact
- Lessons Learned and Remediation
- Nursing Leadership and Collaboration

Learning Objectives

- Describe the impact of a cyber attack
- Discuss the role of nursing informaticists when dealing with a cyber attack
- Outline key takeaways for nurse leaders

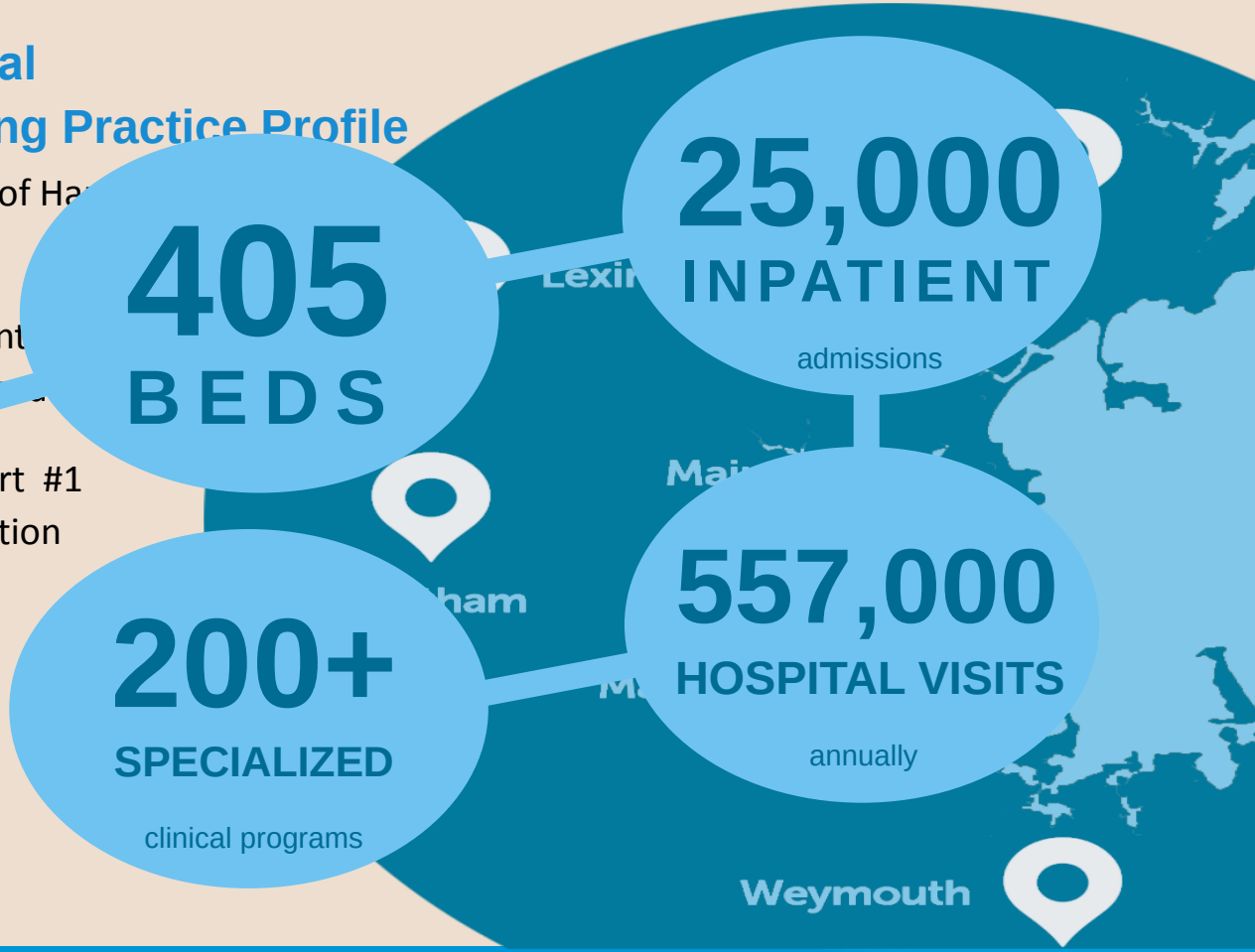
Boston Children's Hospital
Organizational and Nursing Practice Profile

Primary pediatric teaching hospital of Ha
Medical School

World's largest pediatric research ent
leader in translational scientific in

2017-18 U.S. News and World Report #1 ranked Children's Hospital in the nation

- 8 satellite and physician offices
- 7 community hospitals
- 12 community health centers



Lessons Learned from Boston Children's: When Hacktivists Attack Your Hospital

A Shot Across Our Bow

- March 20, 2014 – notified by external cyber intelligence group about Twitter/Pastebin posting by Anonymous, threatening attack
  - result of highly publicized child custody case
  - Anonymous: loose and decentralized group of “hacktivist” individuals
- “d0x” of staff and presiding judge posted
- “Details” of BCH external web site posted

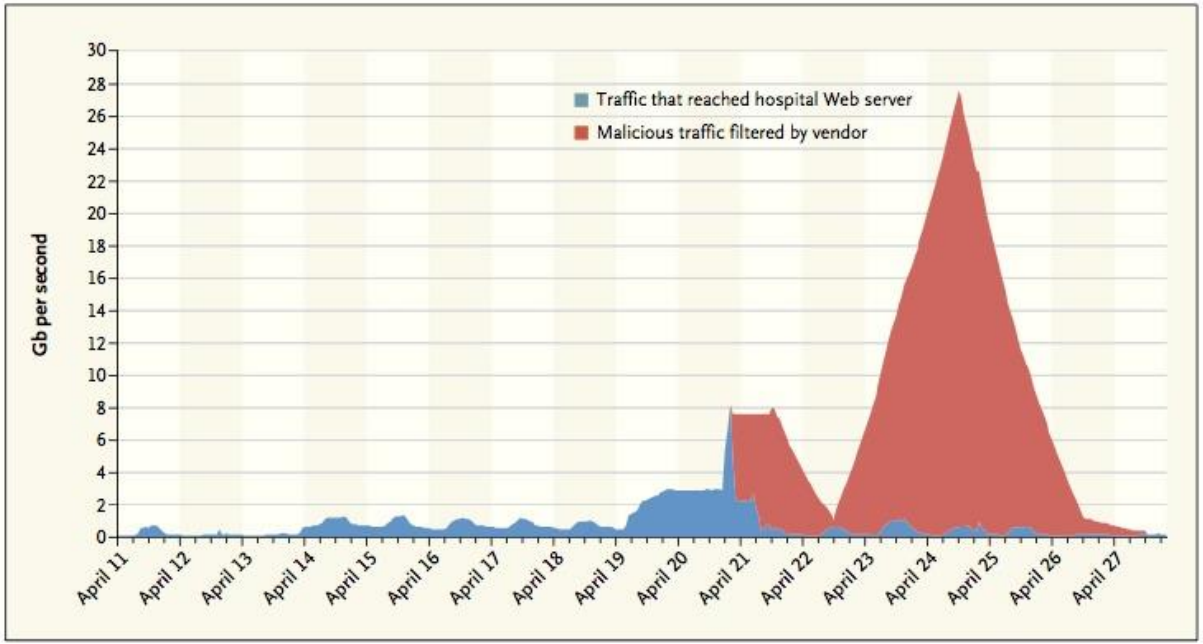
Was This the Real "Anonymous"?

- Not hard to get details they posted
- Not hard to post a video on YouTube
- Should we just discount it then? **NO!!**
- Convened Hospital's Incident Response Team, began forming contingency plans
  - Especially focused on potential need to "go dark", cutting ourselves off from Internet if necessary
- Message to entire organization emphasizing vigilance, email security best practices
- Contacted authorities

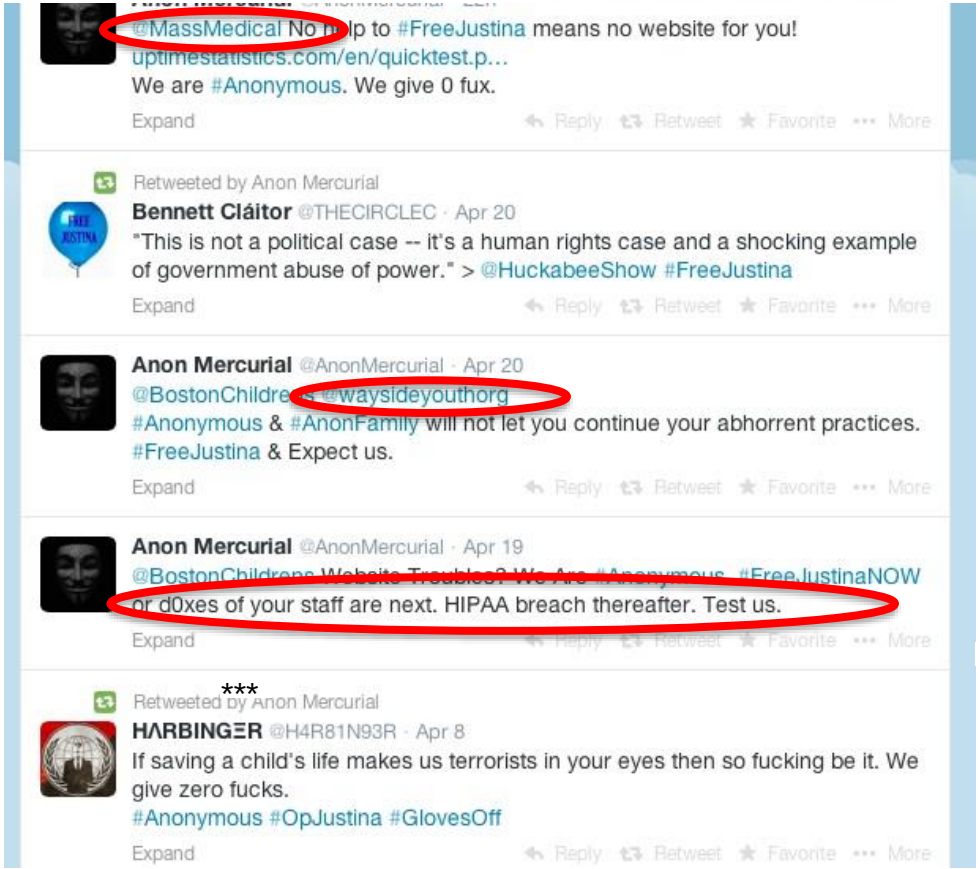
It Begins

- About 3 weeks later... low volume DDoS attack starts
- Mitigated by network changes
- Cat and mouse – we address attack, they change tactic/increase volume
- 1 week later, Easter/Patriot' Day weekend (Boston Marathon bombing 1 year anniversary)
  - Massive uptick in DDoS volume
  - Engaged 3rd party vendor to assist in filtering traffic

Internet Traffic During DDoS Attack



Nigrin, NEJM, July 31, 2014



@MassMedical No help to #FreeJustina means no website for you!
uptimestatistics.com/en/quicktest.p…
We are #Anonymous. We give 0 fux.
Expand Reply Retweet Favorite More

Retweeted by Anon Mercurial

Bennett Cláitor @THECIRCLEC · Apr 20
"This is not a political case -- it's a human rights case and a shocking example of government abuse of power." > @HuckabeeShow #FreeJustina
Expand Reply Retweet Favorite More

Anon Mercurial @AnonMercurial · Apr 20
@BostonChildre[illegible] @waysideyouthorg
#Anonymous & #AnonFamily will not let you continue your abhorrent practices. #FreeJustina & Expect us.
Expand Reply Retweet Favorite More

Anon Mercurial @AnonMercurial · Apr 19
@BostonChildrens Website Troubles? We Are #Anonymous. #FreeJustinaNOW or d0xes of your staff are next. HIPAA breach thereafter. Test us.
Expand Reply Retweet Favorite More

***

Retweeted by Anon Mercurial

HΛRBINGΞR @H4R81N93R · Apr 8
If saving a child's life makes us terrorists in your eyes then so fucking be it. We give zero fucks.
#Anonymous #OpJustina #GlovesOff
Expand Reply Retweet Favorite More

Not Just DDoS…

- Direct penetration attacks on exposed ports, web sites
  - Proactively took down virtually all externally facing sites: research, philanthropy, patient and provider portals, etc…
- Massive influx of malware laden emails
  - Proactively shut down entire email system for ~24 hrs
  - Re-emphasized to staff to not open suspicious mails/attachments
  - Ensured no malware made it through filters
- Re-contacted authorities – advised no press!

BRUINS WIN IN OVERTIME, 3-2, PUSH RED WINGS TO THE BRINK — C1

The Boston Globe

FRIDAY, APRIL 25, 2014

In the news

Late shift

Friday: Turning rainy at night; high 58-63, low 41-46

Saturday: Rainy, cooler; high 47-52, low 39-44

High tide: 8:30 a.m., 9:04 p.m.

Sunrise: 5:48 Sunset: 7:37

Complete report, **B13**

Cyberattack hits Children's Hospital

May be the work of group opposing teen's treatment

By Michael B. Farrell and Patricia Wen
GLOBE STAFF

The infamous computer hacker network known as Anonymous threatened to attack Boston Children's Hospital over the child custody case involving Justina Pelletier last month, just a few weeks before the medical center's website was subjected to numerous cyberassaults.

The anti-authority members of Anonymous sometimes appear in Guy Fawkes masks.

Anonymous has made its interest in the case clear. Several weeks ago, the group claimed responsibility for an attack on the website of Wayside Youth and Family Support Network, the Framingham residential facility where 15-year old Justina has been living since January under state custody.

After the more recent attack on Children's, some patients and medical personnel could not use their online accounts to check appointments, test results, and other case information after the hospital shut down those Web pages.

The threats from Anonymous are the latest to emerge against

Firefigl deal wo raise pa by 18.8

City's 6-year p put at $92.4m is expected ne

By Meghan E. I


Anonymous
@YourAnonNews
Supports digital and AFK activists.
Right behind you. · youranonnews.org
TWEETS
91.2K
FOLLOWING
643
FOLLOWERS
1.24M
Follow
Anonymous @YourAnonNews 8h
To all the "Anons" attacking the CHILDREN'S HOSPITAL in the name of Anonymous - IT IS A HOSPITAL: STOP IT.
Expand
Reply
Retweet
Favorite


EXPECT US.
TWEETS
13
FOLLOWING
6
FOLLOWERS
6
Follow
Tweets
Anon Mercurial @AnonMercurial · 22h
@NSTAR_News We advise you to stop helping Boston Children's Hospital if you like your website to work: uptimestatistics.com/en/quicktest.p...

It Ends

- About 1 week after high volume DDoS started, it abruptly declined, to a low trickle
- Only gradually brought externally facing sites back online, after extensive 3rd party (re)penetration testing
- Took a deep breath!

Out of all bad things...
…good things come

The NEW ENGLAND JOURNAL of MEDICINE

Perspective
JULY 31, 2014

When 'Hacktivists' Target Your Hospital

Daniel J. Nigrin, M.D.

Earlier this year, Boston Children's Hospital was targeted in a sustained cyberattack purportedly instigated by the hacker group known as Anonymous. With cybersecurity becoming an increasingly im-

mation about the hospital's public-facing website, suggesting that it might become a target.

Several weeks later, the hospital began to experience a low-level "distributed denial of ser-

What Did We Learn

- DDoS countermeasures are critical!
- Know what systems (or features within systems) depend on Internet access, and have contingency plans for those
- Recognize importance of email, and need for alternate forms of communication
- Need to push through security initiatives – no excuses anymore
- Securing teleconference meetings
- Separating signal from noise

And Most Importantly

As an industry, we've got to pay closer attention to these threats, and prioritize our efforts against them, **far more** than we have done in the past.

Postscript – Could it Happen Again?

CBS Detroit

FOLLOW US

Home News Health Sports Best Of Watch+Listen Events Weather Traffic Directory Travel Deals Autos

Latest News Local Politics Business Tech Autos Health National World Galleries

Flint Hospital Falls Victim To 'Cyber Attack' Day After Hacking Group Anonymous Launches Crusade For Justice In Water Crisis

January 22, 2016 6:54 AM

Filed Under: anonymous, Computer Hacking, flint, Flint Water, Flint water crisis, Hurley Medical Center

FLINT (WWJ) – A hospital in Flint is confirming it was the victim of a "cyber attack," just a day after hacking group Anonymous released a video targeting those they feel are to blame for the water fiasco.

WATCH & LISTEN

FOLLOW US ON

Postscript #2

Menu | Metro | SUBSCRIBE NOW Get unlimited access to Globe.com for only 99¢ | Subscribe Starting at 99 cents

Somerville man accused of cyberattack on hospital picked up off Cuban coast

By Steve Annear | GLOBE STAFF FEBRUARY 17, 2016

A Somerville man who allegedly launched a cyberattack on a local hospital's website under the name of the hacker network Anonymous was picked up off the coast of Cuba this week when his boat experienced trouble on the open seas, federal prosecutors said.

Martin Gottesfeld, 31, was arrested by federal officials after he came ashore in

Top 10 Trending Article

Most Viewed | Most Commented

Officials search Boston Harbor f
Harvard man

A father's worry, as his son goes

At UVM, substance-free dorm c
personal trainer, nutrition coach

Donald Trump makes himself gr
with help from Jeb and W

Baby boomer retirements may s
economic growth

Boston Globe, February 17, 2016

Postscript #3

ANONYMOUS HACKER INDICTED AS HUNGER STRIKE CONTINUES

BY ANTHONY CUTHBERTSON ON 10/21/16 AT 12:42 PM

TECH & SCIENCE ANONYMOUS

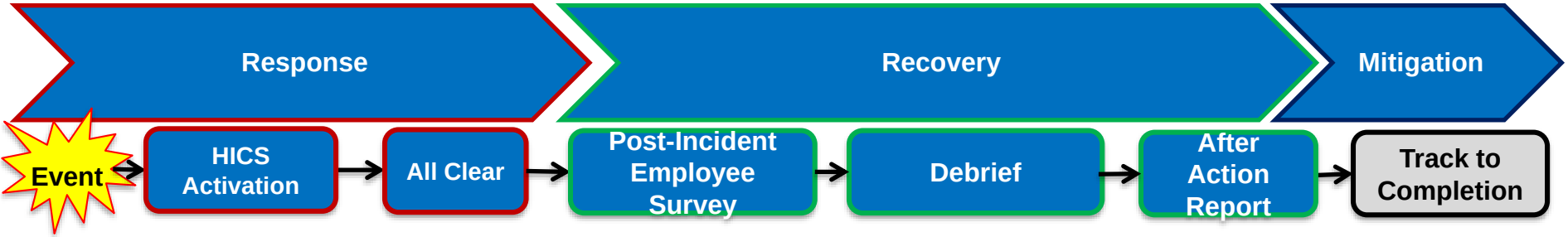
A member of Anonymous has been indicted on hacking charges whilst on the third week of a prison hunger strike protesting perceived institutionalized torture and political prosecutions.

Martin Gottesfeld, 32, was charged this week in relation to the hacking of Boston Children's Hospital in 2014 following the alleged mistreatment of one of its patients. Gottesfeld has previously admitted to targeting the

Gottesfeld pictured in 2010. (Facebook)

Newsweek.com, October 21, 2016

Parallels with Prolonged EHR Downtime



Response

March 2015

Hospital Incident Command System (HICS) activation in Command Center activated for multiple days

Recovery

March – June 2015

Multiple debriefs conducted
System-wide employee survey

After Action Report created

Numerous Action Items Identified

Mitigation

July 2015-Present

Internal plan of correction spanned >24 departments

Remote hosting implementation

High reliability cultural transition

Downtime Prevalence

From the literature:

- 96% of institutions reported at least one unplanned downtime (of any length) in the last 3 years
- 70% had at least one unplanned downtime greater than 8 hours in the last 3 years
- Three institutions reported that one or more patients were injured as a result of either a planned or unplanned downtime
- The majority of institutions (70–85%) had implemented some useful practices, but very few practices were followed consistently

“Contingency planning for electronic health record-based care continuity: A survey of recommended practices” Dean F. Sittig, Daniel Gonzalez, Hardeep Singh. International Journal of Medical Informatics, July 2014

Pharmacy and Lab Workflow

Orders Submitted

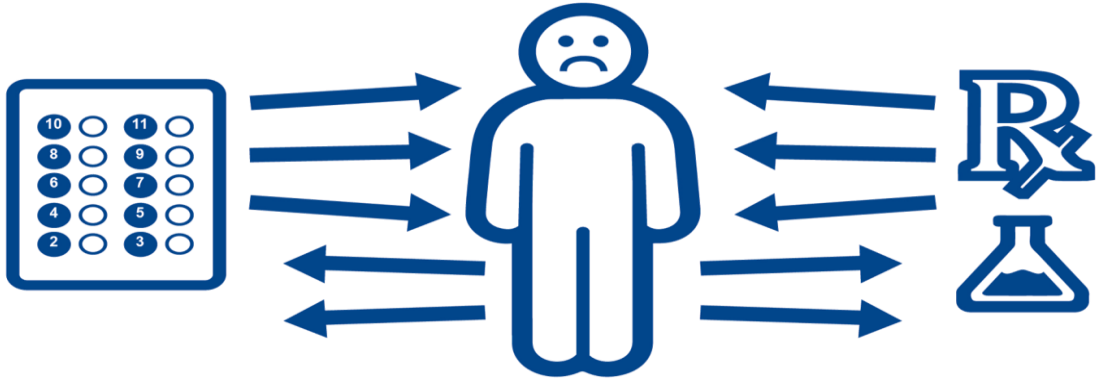
Floors

Pharmacy/Lab

Orders Completed

Pharmacy and Lab Workflow

Floors



Pharmacy/Lab

The Recovery Process

- The plan for recovery starts at the beginning of the downtime.
- Staffing plans to support downtime and recovery need to be developed by managers and supervisors within the first 24 hours of downtime.
- Once system is repaired and ready to be given back to end-users, interdisciplinary teams will need to ensure documentation of historical information. This could take up to 4 to 8 hours.

Lessons Learned and Remediation

Pharmacy Operations

Pain Points

- Delays in Medication orders and delivery
- Lack of medication tracking
- Medication safety
- Staff overworked and exhausted

Remediation

- Established dedicated phone line for stat orders and requests
- Revised medication request process
- Increased number of fax machines
- Used runners
- Created staff phone list and call-in tree
- Created an electronic database to track new order entries, refills and label generation

Laboratory Medicine

Pain Points

- Variability/errors/ambiguity in paper requisitions
- Decreased productivity/ throughput
- Increased turnaround time for test results
- Inability to ensure prompt receipt of results to providers

Remediation

- Collected and phased out old paper requisitions
- Created new, simplified paper requisitions
- Limiting testing done during downtime
- Designed downtime-specific staff roles
- Standardized process for delivery of lab results during downtime

Documentation and Health Information Management

Pain Points

- Staff inexperience with paper documentation
- Old documentation forms being used
- Delays in billing due to coding
- Documentation from downtime had many compliance issues (i.e. missing dates, times and/or signature, etc.)
- Potential for duplicate documentation

Remediation

- Revised/standardized downtime paperwork
- Designed “Downtime Code Carts”
- Prepared an annual downtime education for all clinical staff
- Outdated form removal

Patient, Family, and Staff Communication

Pain Points

- Frontline staff needed more support in talking with patients/families about the downtime event
- Inconsistent methods of communication

Remediation

- Created scripting for communicating with patients/ families
- Created a family education
- Developed a way to take a quick “pulse” of staff’s communication needs
- Designed key message templates
- Created a just-in-time training to coach staff

Creating a Downtime Binder

- Prescriber Order Forms
- Medication Administration Record (MAR)
- Nursing Admission Assessment (NAA)
- Progress Notes
- Inpatient and Critical Care Flow Sheet
- Management Plans
- Blood Bank Requisition and Lab Order Sheet
- Discharge Plan, Summary, and Additional Instructions
- Documentation policies
- Sample orders
- Sample Prescriptions (including DME)
- Reminder to use downtime order sets
- Directions for documentation of medications
- Guidelines for completing requisitions
- Area downtime preparedness checklist
- Medication History form

Impacts beyond the EHR

- Paging and communication systems
- Online drug formulary
- Custom applications
- Polices & Procedures
- Web-based clinical resources
- Research databases/registries
- Patient food ordering
- Lab instrument interfaces

Focused Education

- How to use a paper flow sheet and paper Medication Administration Record (MAR)
- Prescriber guidelines for an EHR downtime
- Ordering during downtime
  - Essential components of an order
  - Prescriptions during downtime
  - Order re-entry during downtime recovery
- Documentation during downtime and recovery

How can staff be prepared?

Ensure staff know:

- Institution's Patient Documentation policy
- How to print and use downtime paperwork
- Where downtime forms and supplies are
- Communication protocols
- **Resources for getting more information**

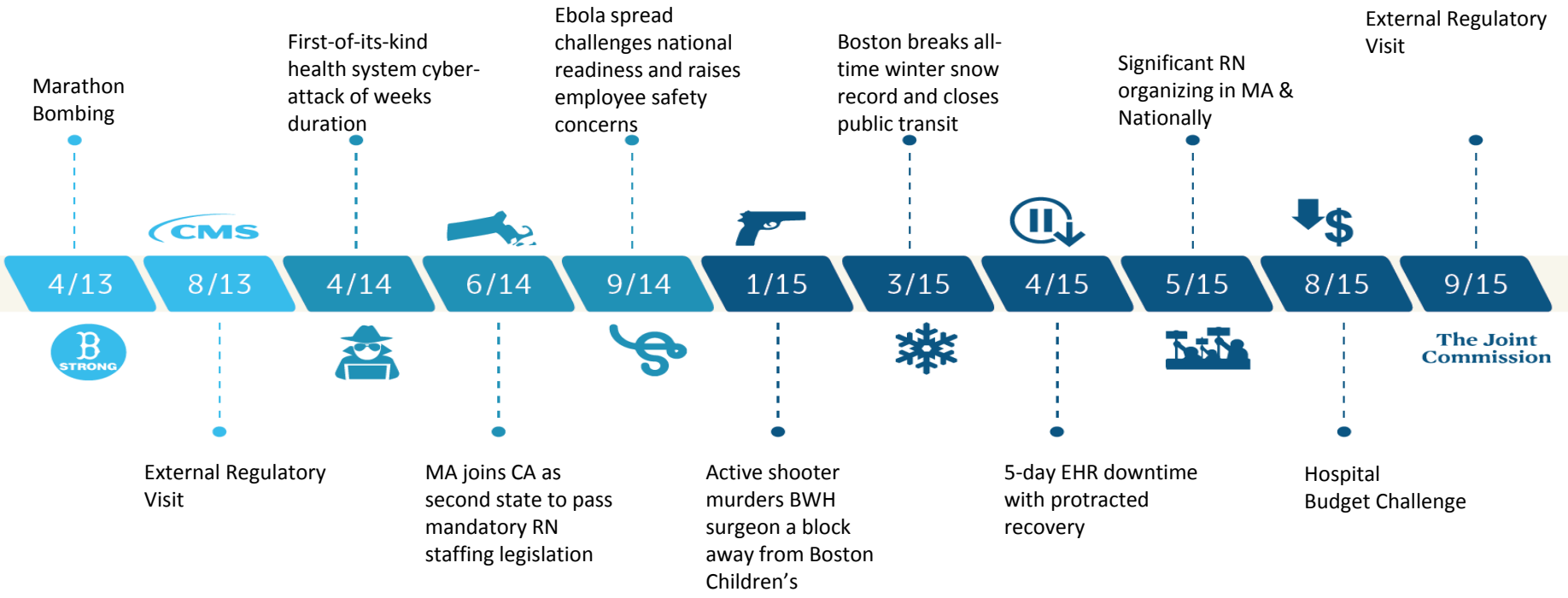
The Silver Lining

What we thought went well:

- Experienced staff taught newer staff how to chart on paper
- Increased communication between doctors and nurses
- Patient and family communication
- Command Center communication and availability was helpful
- ***Event brought staff together and fostered team work***

Nurse Executive Perspective

Impacts to Boston Children's Work Environment: 2013–2015



CNO & Executive Leadership Insights

- Employee heroics vs system capabilities: Cumulative system and human stressors
- Marshalling Senior Clinical Leadership Committee guidance early and often
- Making capacity management decisions – balancing safety, quality, access, and employee considerations
- Internal and external communication – media, employees, and patients & families
- High Reliability: A cultural shift to focus on error prevention, transparency, and situational awareness

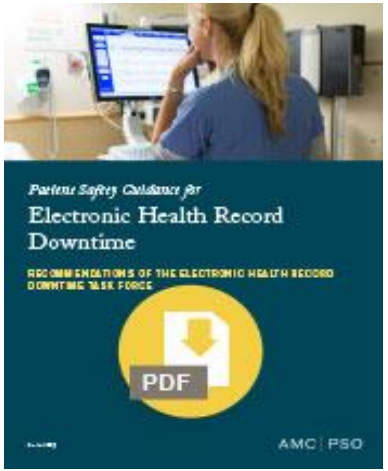
Importance of Hospital Incident Command

- The Hospital Incident Command System is used to organize direct responders during a hospital emergency.
- It allows for overall site management, for real-time decision-making, and for a clearly-defined reporting structure.
- Boston Children's uses this system in a variety of situations – from winter weather response to IT downtimes to citywide events like the Boston Marathon bombings.
- Important to identify clearly for staff what is and is not happening in a given situation.

90-day Internal Post Event Review & External Patient Safety Organization (PSO) Collaboration

- Collaboration with Controlled Risk Insurance Corporation (CRICO) to convene the organization's Academic Medical Center Patient Safety Organization (AMC PSO) as established under the Patient Safety and Quality Improvement Act of 2005
- Creation of Electronic Health Record Downtime white paper

https://www.rmf.harvard.edu/Clinician-Resources/Guidelines-Algorithms/2017/EHR-Downtime-Guidelines



High Reliability is…

- An enterprise-wide commitment to doing things right the first time, every time
- A cultural shift to focus on error prevention, transparency, and situational awareness
- 5 Principles:
  - Preoccupation with failure
  - Reluctance to simplify interpretations
  - Sensitivity to operations
  - Commitment to resilience
  - Communication at all levels
- Goal: zero serious events of preventable harm

AT BOSTON CHILDREN'S HOSPITAL
EVERY MOMENT MATTERS

Questions

Sara Gibbons, MSN, RN-BC, CPN

Sara.Gibbons@childrens.harvard.edu | @saragibbons13 | https://www.linkedin.com/in/sara-gibbons/

Daniel Nigrin, MD, MS

Daniel.Nigrin@childrens.harvard.edu | @dnigrin | https://www.linkedin.com/in/danielnigrin/

Laura Wood, DNP, MS, RN, NEA-BC

Laura.Wood@childrens.harvard.edu | @LJWood01 | https://www.linkedin.com/in/laura-j-wood/

* Note of appreciation to our colleague Marcie Brostoff, MS, RN, NE-BC, Vice President & ACNO for her leadership in advancing this work