Tactical and Practical Incident Response in the Cybersecurity Age

HIMSS

CENTRAL & SOUTHERN OHIO Chapter

Nationwide Children's Hospital… a Complex Organization

- 1.2 Million annual visits
- 60+ locations
- > 15k user accounts
- More than a hospital
- HIPAA, FISMA, PCI, FDA and other compliance requirements

So…things can happen!

[redacted]

And NCH is not alone!

- The total number of reported data breaches reached an all time high of 3,930 in 2015, exposing over 736 million records. (https://blog.datalossdb.org/analysis/)

- 2015 healthcare security breaches: a long list (http://www.healthcareitnews.com/slideshow/2015-healthcare-security-breaches-long-list)

Healthcare IT News

- As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format…(83 in Q1 2016)

HHS.gov
Office for Civil Rights

Incident Response is a MUST Have!

1. Fulfills a compliance requirement
2. Minimizes the Impact of an event to the organization
3. Protects the organization and the brand
4. Communicates with customers
5. Facilitates people knowing their role
6. Brings impacted services back online ASAP

Objectives

- Understand key roles and relationships within the incident response team as well as how the incident response team should relate to C-level governance structures

- Gain insights and ideas to effectively test the incident response team and incorporate the lessons learned into the incident response program

- Come away with some concrete ideas on how to make an incident response plan actionable

Agenda

- Preparation*
  - Incident response teams
  - Governance, roles & responsibilities
  - Testing the response
- Detection & Analysis
- Containment, Eradication, and Recovery
- Post-Incident Activity*
  - Breach Analysis

* Focus Areas

Preparation

Getting Started

- Use a framework & guidance! - NIST 800-61 Computer Security Incident Handling Guide
- Build relationships with key roles
- Share knowledge and discuss industry events. What if that happened HERE??
- Be Satisfied with progress, because it won't be perfect!
- Everybody loves "the dirt"

Incident Response Teams

Incident Response Team Roles and Responsibilities

Information Security Officer

- Team coordination and IR plan development
- reporting incidents to governance team
- Ensuring security related incidents are managed effectively

Privacy Officer

- Providing guidance on issues related to privacy
- Developing appropriate communication to impacted parties
- Ensuring privacy related incidents are managed effectively

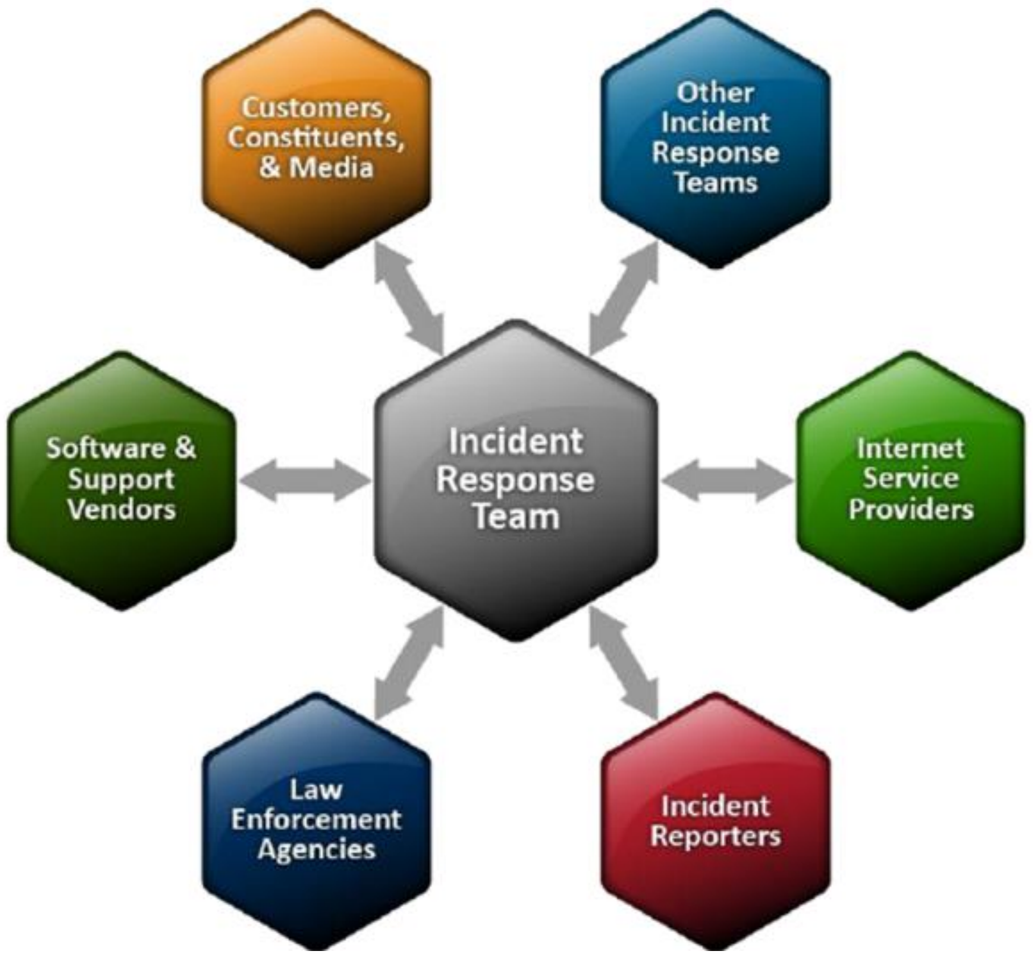
Legal

- Ensuring legal obligations are met
- Ensuring regulation is properly interpreted and implemented

Incident Response Team Roles and Responsibilities

Compliance	• Ensuring compliance obligations are met • Ensuring reporting is effective • Ensuring incidents are treated with consistency
HR	• Providing guidance regarding personnel issues
Public Relations/ Communication	• Communicating appropriate corporate messaging to internal and external parties
Physical Security	• Providing physical security capability • Facilitating communication to the CPD
Clinical	• Ensuring clinical staff is considered in all aspects of incident response
Research	• Ensuring the research institute is considered in all aspects of incident response

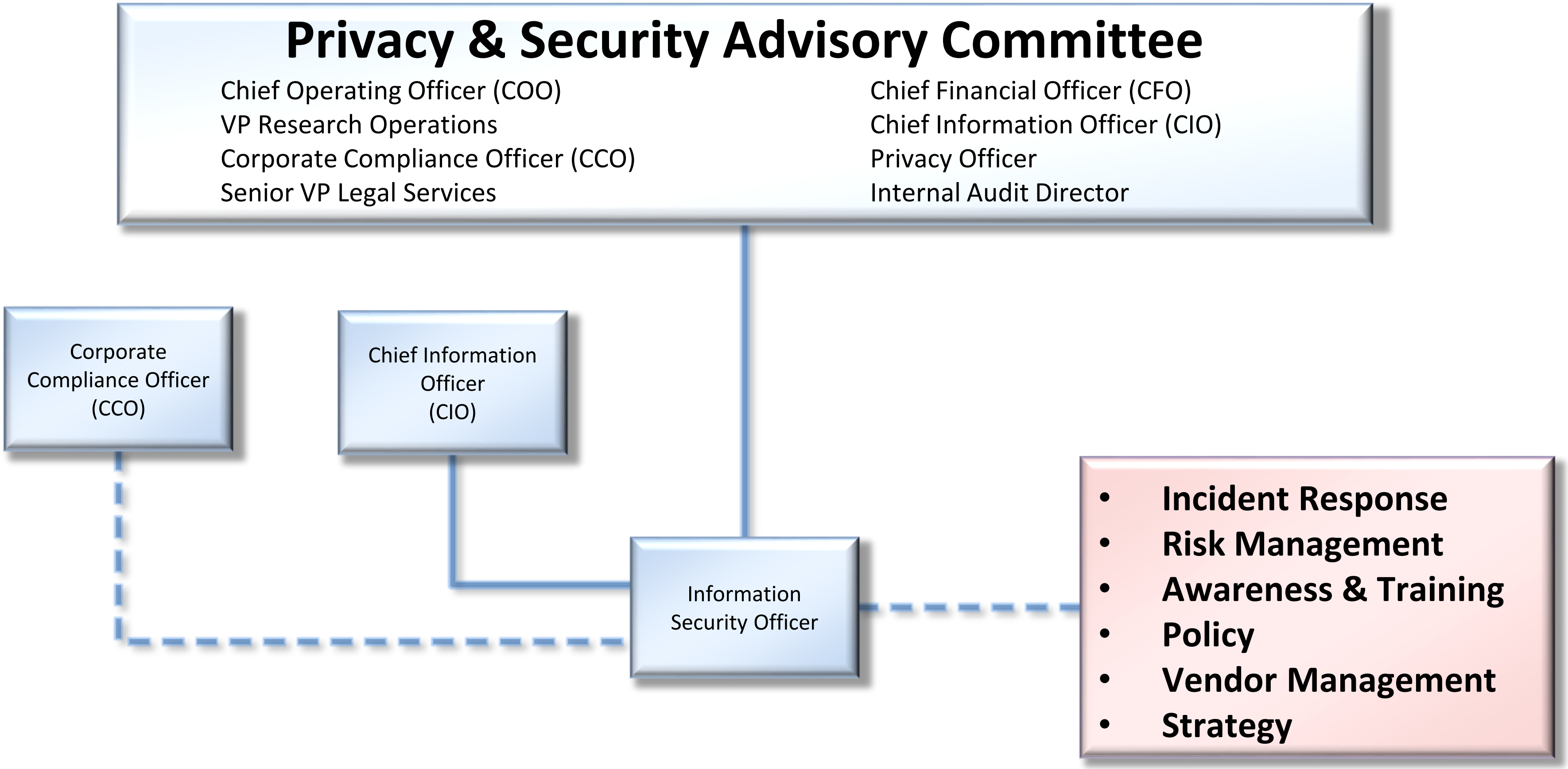
External Team


Customers, Constituents, & Media
Other Incident Response Teams
Software & Support Vendors
Incident Response Team
Internet Service Providers
Law Enforcement Agencies
Incident Reporters

Technical Incident Response

- Privacy and Confidentiality expectations
- Small teams with broad knowledge – reach out to SME as needed
- Tech team need training too
  - Right sizing security
  - Chain of Custody
  - Current events
  - Red Team practice
- Tools and governance
- Communication

Governance



Privacy & Security Advisory Committee

Chief Operating Officer (COO)
VP Research Operations
Corporate Compliance Officer (CCO)
Senior VP Legal Services

Chief Financial Officer (CFO)
Chief Information Officer (CIO)
Privacy Officer
Internal Audit Director

Corporate Compliance Officer (CCO)

Chief Information Officer (CIO)

Information Security Officer

- **Incident Response**
- **Risk Management**
- **Awareness & Training**
- **Policy**
- **Vendor Management**
- **Strategy**

Test the teams

The following is a scenario created by the information security team at Nationwide Children's Hospital for the sole purpose of testing the incident response team. None of these incidents are real, but they are realistic.

Assign a clear owner

Provide Guardrails

Expect Excellence

Expect Creativity

Present a Scenario…and provide time to react !

Listen carefully, I represent an organization that has acquired significant amount if information from your hospital over several weeks. We require a payment from you to us in the amount of $5M. If you are willing to comply place a 1 inch solid black star in the upper right corner of your home page at nationwidechildrens.org. Contact will be made will be made with money transfer information at that time. Do not involve the police and do not ignore us. You have 8 hours.

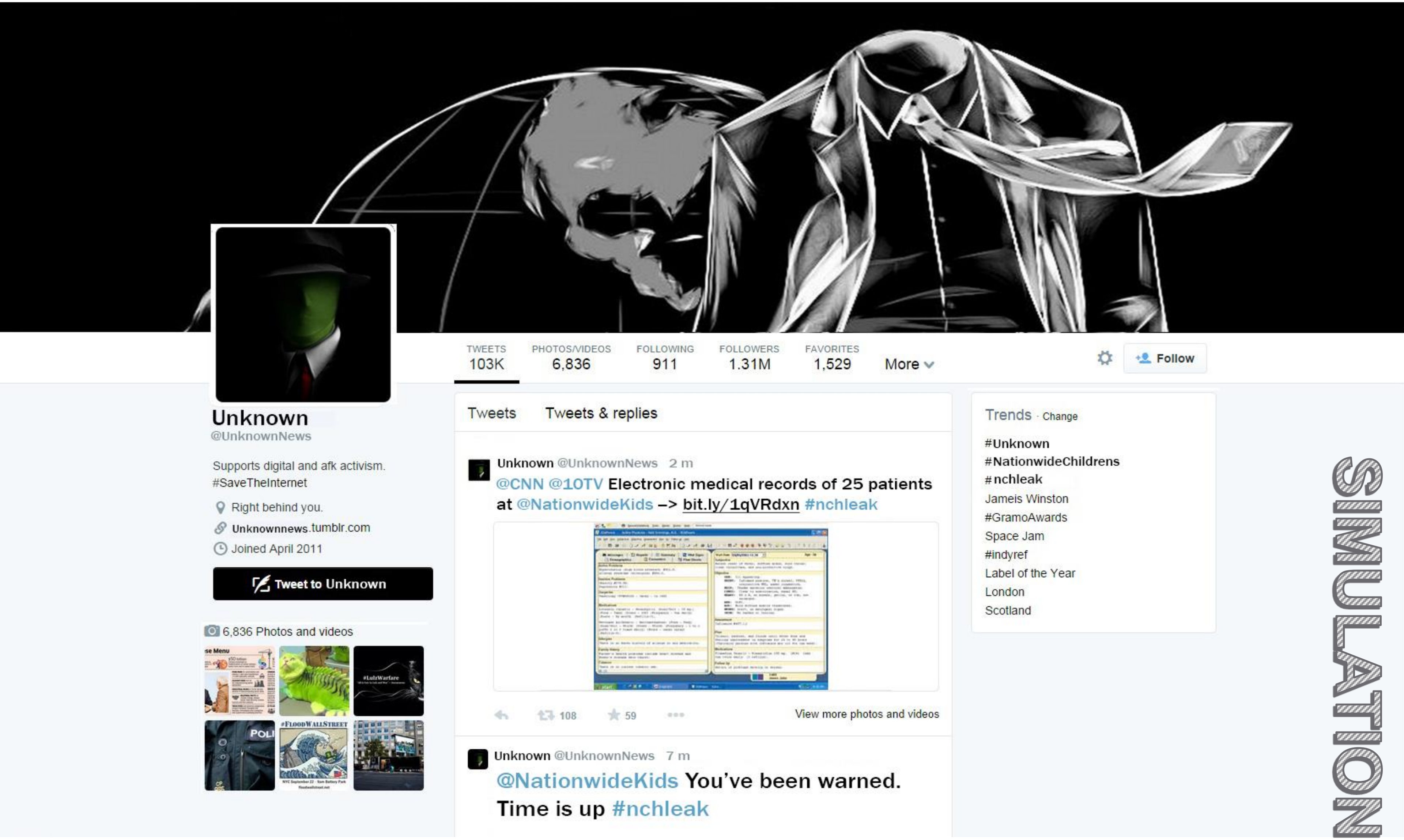
SIMULATION

Add some Time Pressure

You have not yet complied with our demands. If you chose not to we will release the 17,387 records in our possession onto the internet. To show you that we're serious we have already released 25 of them for public viewing. You have one hour.

SIMULATION

Add Some New Information…make it real!



Unknown
@UnknownNews

Supports digital and afk activism. #SaveTheInternet

Right behind you.

Unknownnews.tumblr.com

Joined April 2011

Tweet to Unknown

6,836 Photos and videos

TWEETS	PHOTOS/VIDEOS	FOLLOWING	FOLLOWERS	FAVORITES
103K	6,836	911	1.31M	1,529

Unknown @UnknownNews 2 m
@CNN @10TV Electronic medical records of 25 patients at @NationwideKids –> bit.ly/1qVRdxn #nchleak

108 59 View more photos and videos

Unknown @UnknownNews 7 m
@NationwideKids You've been warned. Time is up #nchleak

Trends · Change

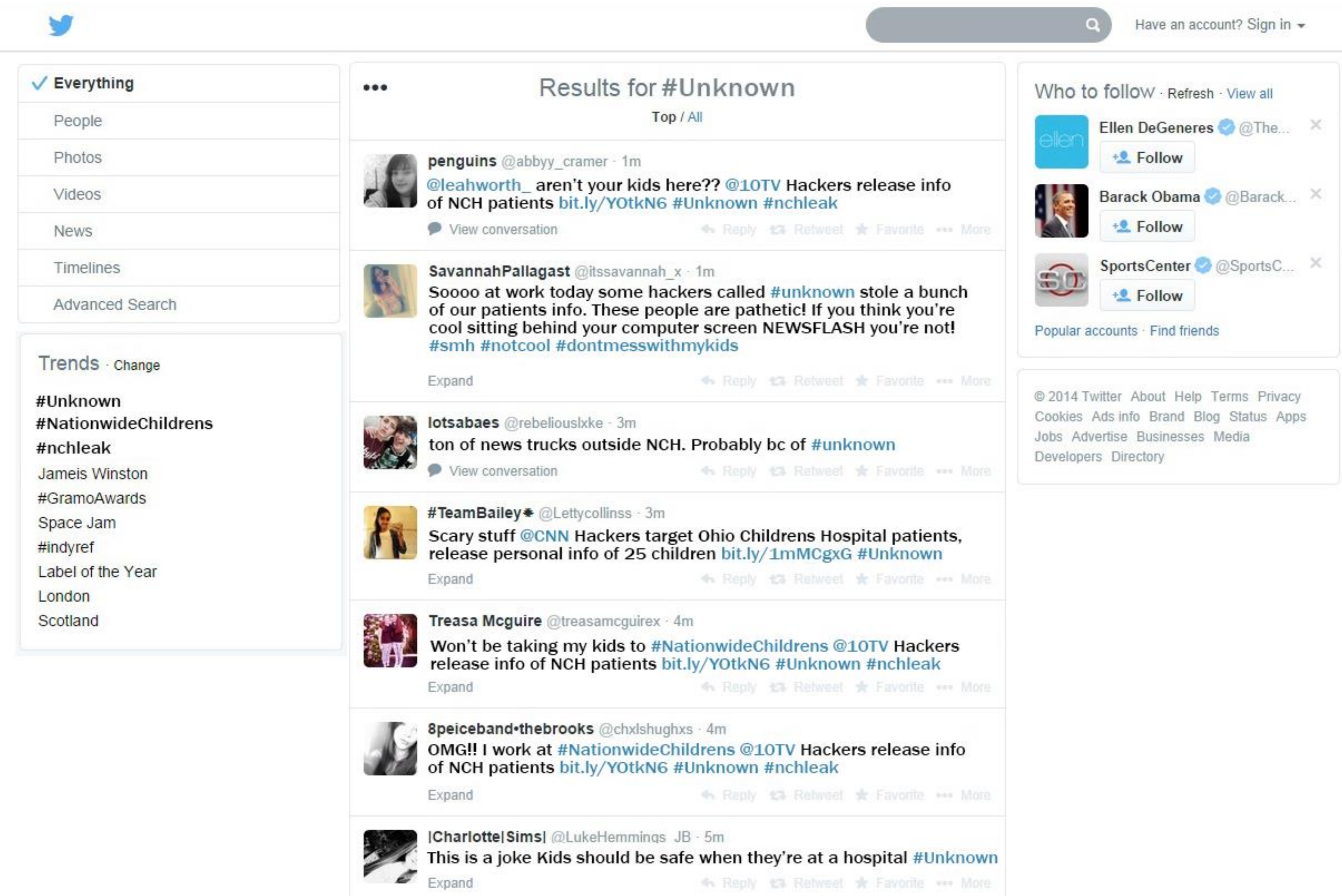
#Unknown
#NationwideChildrens
#nchleak
Jameis Winston
#GramoAwards
Space Jam
#indyref
Label of the Year
London
Scotland

SIMULATION

Add a dash of Media…and some more information.

SIMULATION

Add a social media component, and create the need to escalate!



Results for #Unknown

Top / All

penguins @abbyy_cramer · 1m
@leahworth_ aren't your kids here?? @10TV Hackers release info of NCH patients bit.ly/YOtkN6 #Unknown #nchleak
View conversation · Reply · Retweet · Favorite · More

SavannahPallagast @itssavannah_x · 1m
Soooo at work today some hackers called #unknown stole a bunch of our patients info. These people are pathetic! If you think you're cool sitting behind your computer screen NEWSFLASH you're not! #smh #notcool #dontmesswithmykids
Expand · Reply · Retweet · Favorite · More

lotsabaes @rebeliouslxke · 3m
ton of news trucks outside NCH. Probably bc of #unknown
View conversation · Reply · Retweet · Favorite · More

#TeamBailey✸ @Lettycollinss · 3m
Scary stuff @CNN Hackers target Ohio Childrens Hospital patients, release personal info of 25 children bit.ly/1mMCgxG #Unknown
Expand · Reply · Retweet · Favorite · More

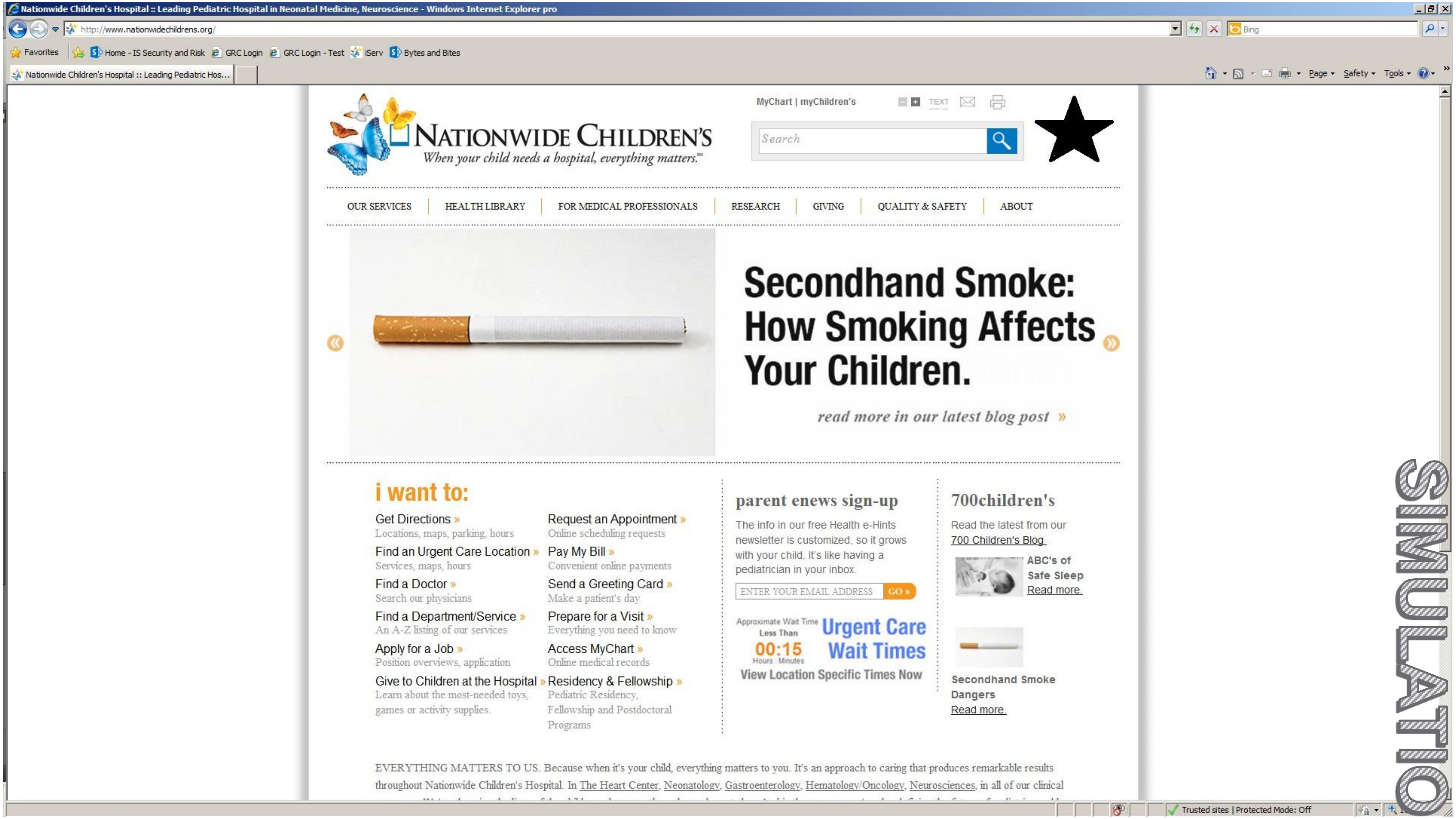
Treasa Mcguire @treasamcguirex · 4m
Won't be taking my kids to #NationwideChildrens @10TV Hackers release info of NCH patients bit.ly/YOtkN6 #Unknown #nchleak
Expand · Reply · Retweet · Favorite · More

8peiceband•thebrooks @chxlshughxs · 4m
OMG!! I work at #NationwideChildrens @10TV Hackers release info of NCH patients bit.ly/YOtkN6 #Unknown #nchleak
Expand · Reply · Retweet · Favorite · More

|Charlotte|Sims| @LukeHemmings JB · 5m
This is a joke Kids should be safe when they're at a hospital #Unknown
Expand · Reply · Retweet · Favorite · More

SIMULATION

Force a Decision



Nationwide Children's Hospital :: Leading Pediatric Hospital in Neonatal Medicine, Neuroscience - Windows Internet Explorer pro
http://www.nationwidechildrens.org/
Bing
Favorites
Home - IS Security and Risk
GRC Login
GRC Login - Test
iServ
Bytes and Bites
Nationwide Children's Hospital :: Leading Pediatric Hos...
Page
Safety
Tools
Trusted sites | Protected Mode: Off

NATIONWIDE CHILDREN'S
When your child needs a hospital, everything matters.℠

MyChart | myChildren's

TEXT

Search

★

OUR SERVICES | HEALTH LIBRARY | FOR MEDICAL PROFESSIONALS | RESEARCH | GIVING | QUALITY & SAFETY | ABOUT

Secondhand Smoke: How Smoking Affects Your Children.

read more in our latest blog post »

i want to:

Get Directions »
Locations, maps, parking, hours

Find an Urgent Care Location »
Services, maps, hours

Find a Doctor »
Search our physicians

Find a Department/Service »
An A-Z listing of our services

Apply for a Job »
Position overviews, application

Give to Children at the Hospital »
Learn about the most-needed toys, games or activity supplies.

Request an Appointment »
Online scheduling requests

Pay My Bill »
Convenient online payments

Send a Greeting Card »
Make a patient's day

Prepare for a Visit »
Everything you need to know

Access MyChart »
Online medical records

Residency & Fellowship »
Pediatric Residency, Fellowship and Postdoctoral Programs

parent enews sign-up

The info in our free Health e-Hints newsletter is customized, so it grows with your child. It's like having a pediatrician in your inbox.

ENTER YOUR EMAIL ADDRESS GO »

Approximate Wait Time
Less Than
00:15
Hours : Minutes
Urgent Care Wait Times
View Location Specific Times Now

700children's

Read the latest from our 700 Children's Blog

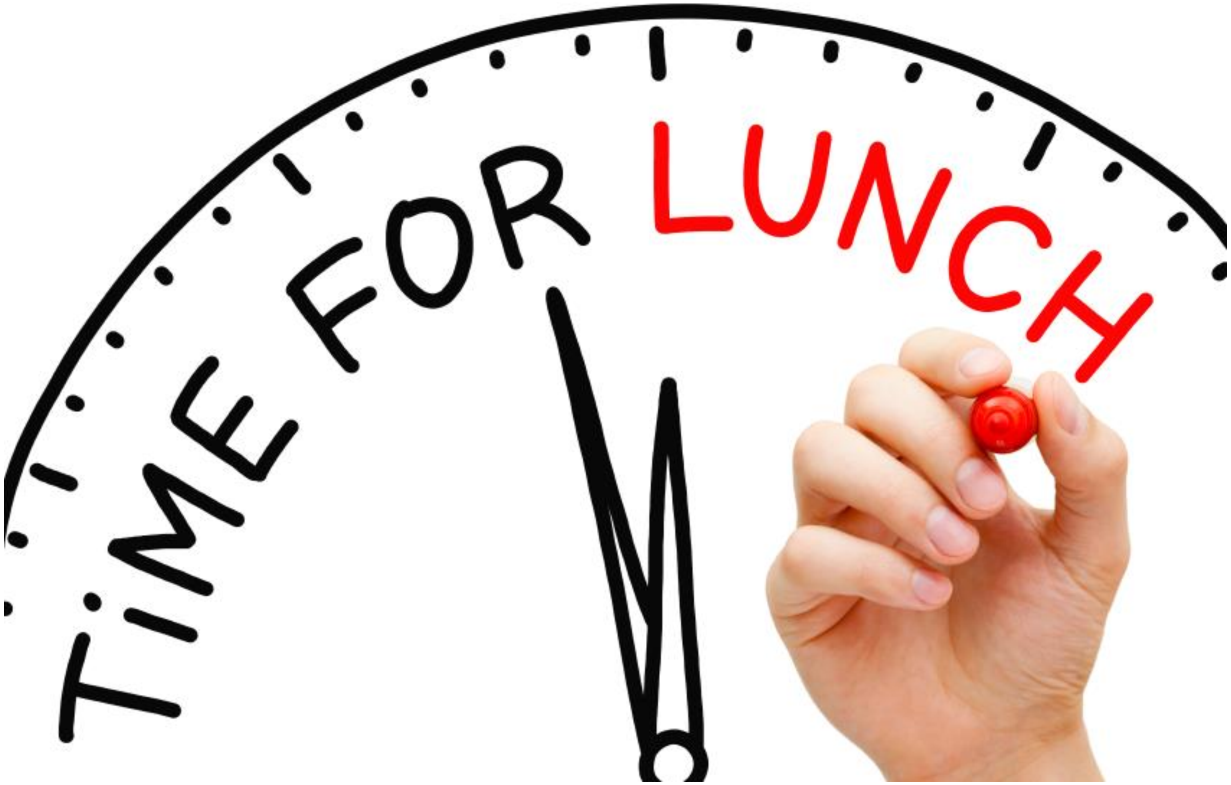
ABC's of Safe Sleep
Read more.

Secondhand Smoke Dangers
Read more.

EVERYTHING MATTERS TO US. Because when it's your child, everything matters to you. It's an approach to caring that produces remarkable results throughout Nationwide Children's Hospital. In The Heart Center, Neonatology, Gastroenterology, Hematology/Oncology, Neurosciences, in all of our clinical

SIMULATION

Serve Lunch



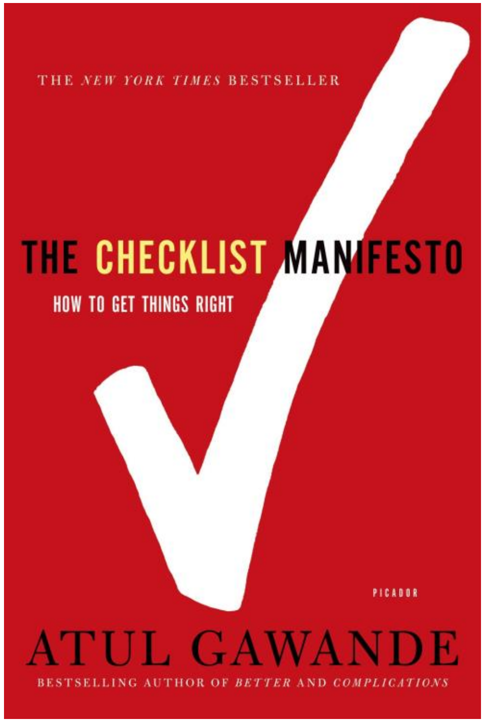
Debrief. Issue After Action Report

- Executive Summary – Share with the governance team
- Major Strengths
- Primary Areas of Improvement
- Areas requiring more education
- Develop content and actions for your next team meetings

SIMULATION

Detection & Analysis

Some Considerations


THE NEW YORK TIMES BESTSELLER
THE CHECKLIST MANIFESTO
HOW TO GET THINGS RIGHT
PICADOR
ATUL GAWANDE
BESTSELLING AUTHOR OF BETTER AND COMPLICATIONS

- What are the likely sources of information in your environment?
- Chain of Custody & eDiscovery
- Who needs to be involved when staff are being interviewed?
- When does a security event turn into a privacy issue?
- Escalation to HICS

Containment Eradication & Recovery

Business Meets Technology - Containment

- Unplug the Internet ???
- Who has authority to make the call?
- Has the incident response team run enough scenarios to understand your organization’s complexity?
- Are you confident your governance team supports you?
- What communication is needed?

Eradication & Recovery

- How do I know it is gone? Use a risk-based approach to decide.
- Can you recover?

Post Incident Activity

A BREACH…

…an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information….[and] is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is

a low probability that the protected health information has been compromised…

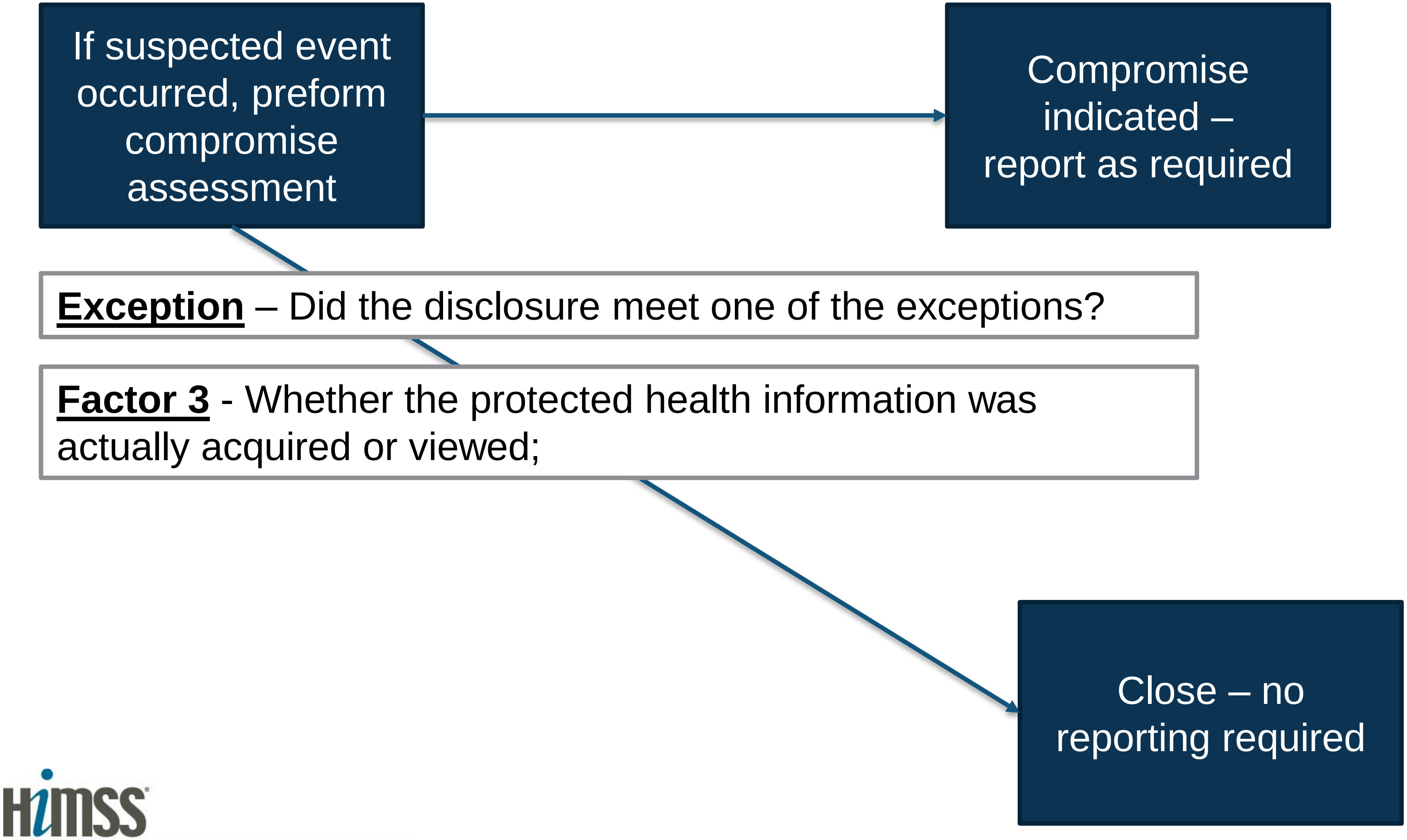
4 Factors of Risk Assessment

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

Exceptions to the definition of “breach.”

1. …unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.
2. …the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
3. …if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

Breach or no Breach?



If suspected event occurred, preform compromise assessment

Compromise indicated – report as required

Exception – Did the disclosure meet one of the exceptions?

Factor 3 - Whether the protected health information was actually acquired or viewed;

Close – no reporting required

Impact Analysis – Factor 1

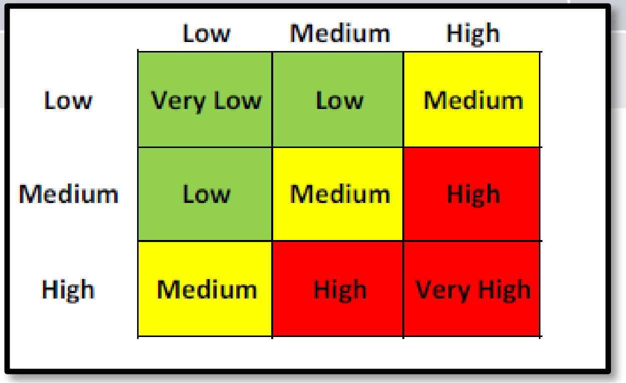
	Financial	Reputational	Personal
High	• ID Theft (SSN, DL, CC)	• Sensitive diagnosis • Employer notified	• Sensitive diagnosis • Revealing photos
Medium	• MRN	• General prescriptions	• Physician's Name
Low	• Publicly available information	• Unidentifiable photo	• Appointment reminder, non-sensitive

Factor 1 - The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification

Likelihood Analysis – Factors 2 & 4

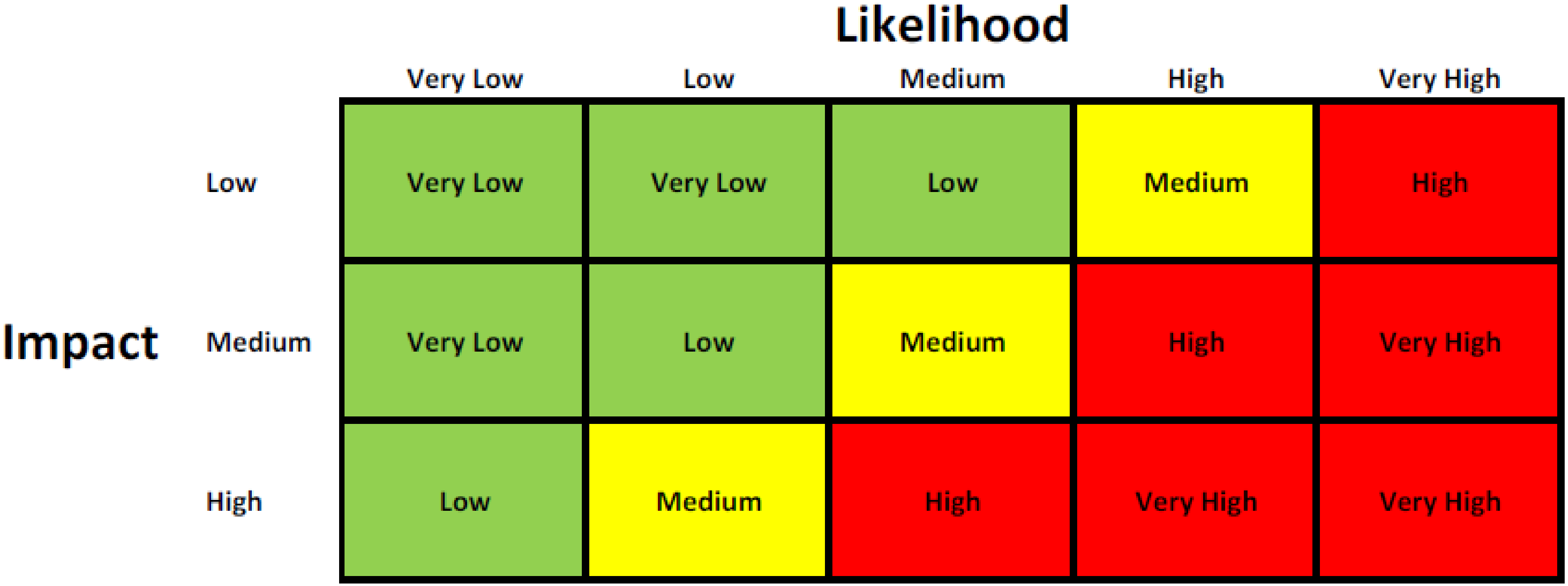
Factor 2 – Who received the PHI:	Likelihood
Covered Entity	Very Low
Business Associate	Low
Inappropriate Access (Snooping)	Medium
Criminal	High
Malicious Intent	High

Factor 4 – Extent risk mitigated	Likelihood
Signed COD	Low
Original Returned	Low
Refuse to sign COD	High
Refuse to return documents	High



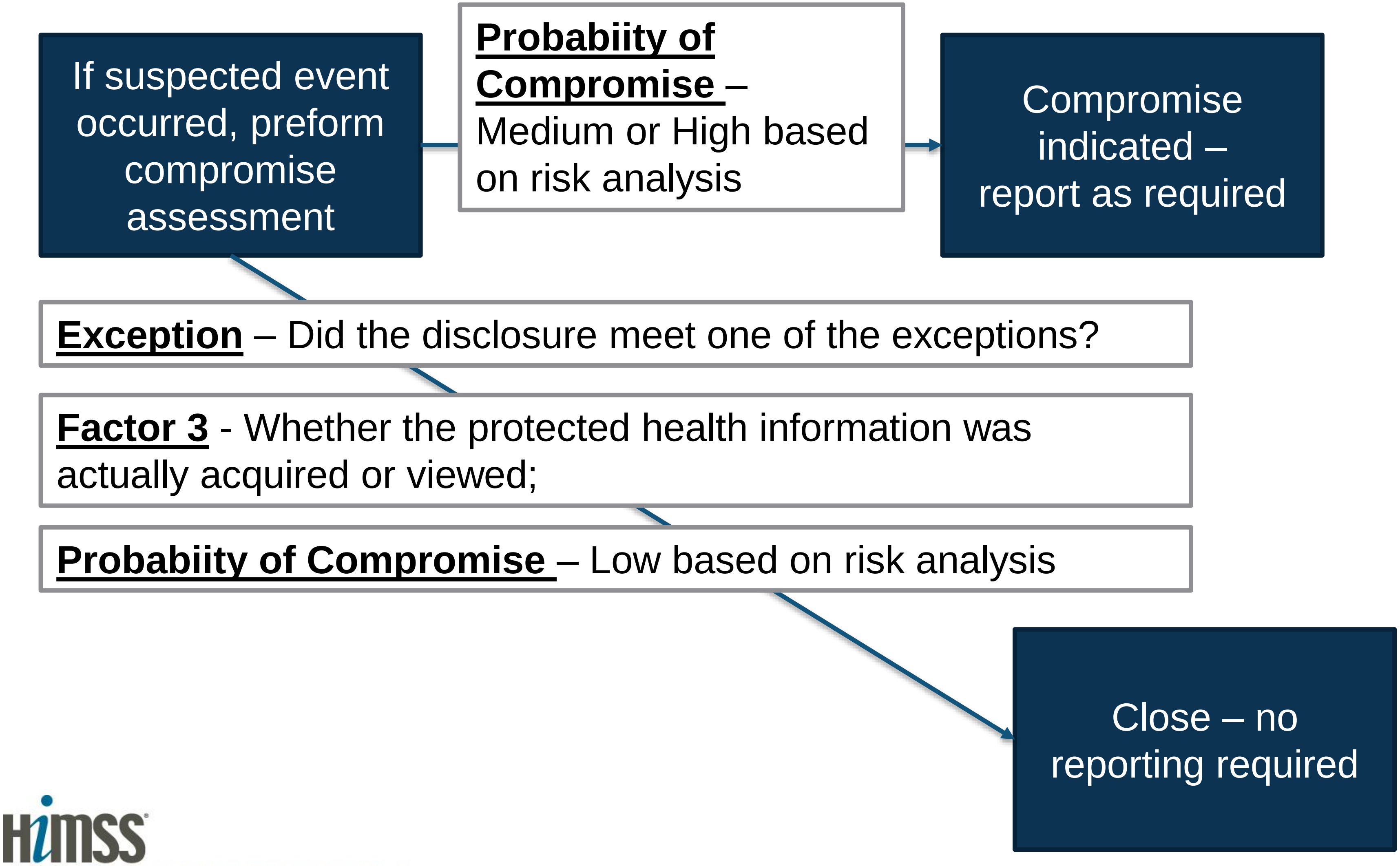
	Low	Medium	High
Low	Very Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	Very High

Probability of Compromise



		Likelihood				
		Very Low	Low	Medium	High	Very High
Impact	Low	Very Low	Very Low	Low	Medium	High
	Medium	Very Low	Low	Medium	High	Very High
	High	Low	Medium	High	Very High	Very High

Breach or no Breach?



If suspected event occurred, preform compromise assessment

Probabiity of Compromise – Medium or High based on risk analysis

Compromise indicated – report as required

Exception – Did the disclosure meet one of the exceptions?

Factor 3 - Whether the protected health information was actually acquired or viewed;

Probabiity of Compromise – Low based on risk analysis

Close – no reporting required

Sniff Test

Next Steps for NCH

- Improve and test our technical incident response teams
- Continue to educate the governance team
- Expand knowledge into middle management tiers
- Monitor and react to “new” threats and environments such as ransomware, zero-day malware, and data in “the cloud”
- Improve consistency in sanctions

Next Steps for Healthcare

- Share your stories – what is working and what is not working
- Higher focus on availability and integrity as a security concern
- Innovative ways to leverage others’ strengths

Brian Baacke

Brian.baacke@nationwidechildrens.org

@BrianBaacke