Tactical and Practical Incident Response in the Cybersecurity Age
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!
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/](https://blog.datalossdb.org/analysis/))


- 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)
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
- 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
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
Listen carefully, I represent an organization that has acquired significant amount of 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 with money transfer information at that time. Do not involve the police and do not ignore us. You have 8 hours.
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.
Add Some New Information... make it real!
Add a dash of Media...and some more information.
Add a social media component, and create the need to escalate!
Force a Decision
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
Detection & Analysis
Some Considerations

• 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, perform 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

<table>
<thead>
<tr>
<th></th>
<th>Financial</th>
<th>Reputational</th>
<th>Personal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High</strong></td>
<td>• ID Theft (SSN, DL, CC)</td>
<td>• Sensitive diagnosis</td>
<td>• Sensitive diagnosis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Employer notified</td>
<td>• Revealing photos</td>
</tr>
<tr>
<td><strong>Medium</strong></td>
<td>• MRN</td>
<td>• General prescriptions</td>
<td>• Physician's Name</td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td>• Publicly available information</td>
<td>• Unidentifiable photo</td>
<td>• Appointment reminder, non-sensitive</td>
</tr>
</tbody>
</table>
**Likelihood Analysis – Factors 2 & 4**

<table>
<thead>
<tr>
<th>Factor 2 – Who received the PHI:</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covered Entity</td>
<td>Very Low</td>
</tr>
<tr>
<td>Business Associate</td>
<td>Low</td>
</tr>
<tr>
<td>Inappropriate Access (Snooping)</td>
<td>Medium</td>
</tr>
<tr>
<td>Criminal</td>
<td>High</td>
</tr>
<tr>
<td>Malicious Intent</td>
<td>High</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Factor 4 – Extent risk mitigated</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signed COD</td>
<td>Low</td>
</tr>
<tr>
<td>Original Returned</td>
<td>Low</td>
</tr>
<tr>
<td>Refuse to sign COD</td>
<td>High</td>
</tr>
<tr>
<td>Refuse to return documents</td>
<td>High</td>
</tr>
</tbody>
</table>
# Probability of Compromise

<table>
<thead>
<tr>
<th>Impact</th>
<th>Very Low</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Medium</td>
<td>Very Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
</tr>
</tbody>
</table>
Breach or no Breach?

If suspected event occurred, preform compromise assessment

**Probability 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;

**Probability 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](mailto:Brian.baacke@nationwidechildrens.org)
[@BrianBaacke](https://twitter.com/BrianBaacke)