Hollywood's Hype and the Harsh Reality of a Ransomware Attack

Dave Dillehunt
Vice President & CIO
FirstHealth of the Carolinas

Clyde Hewitt
Vice President, Security Strategy
CynergisTek

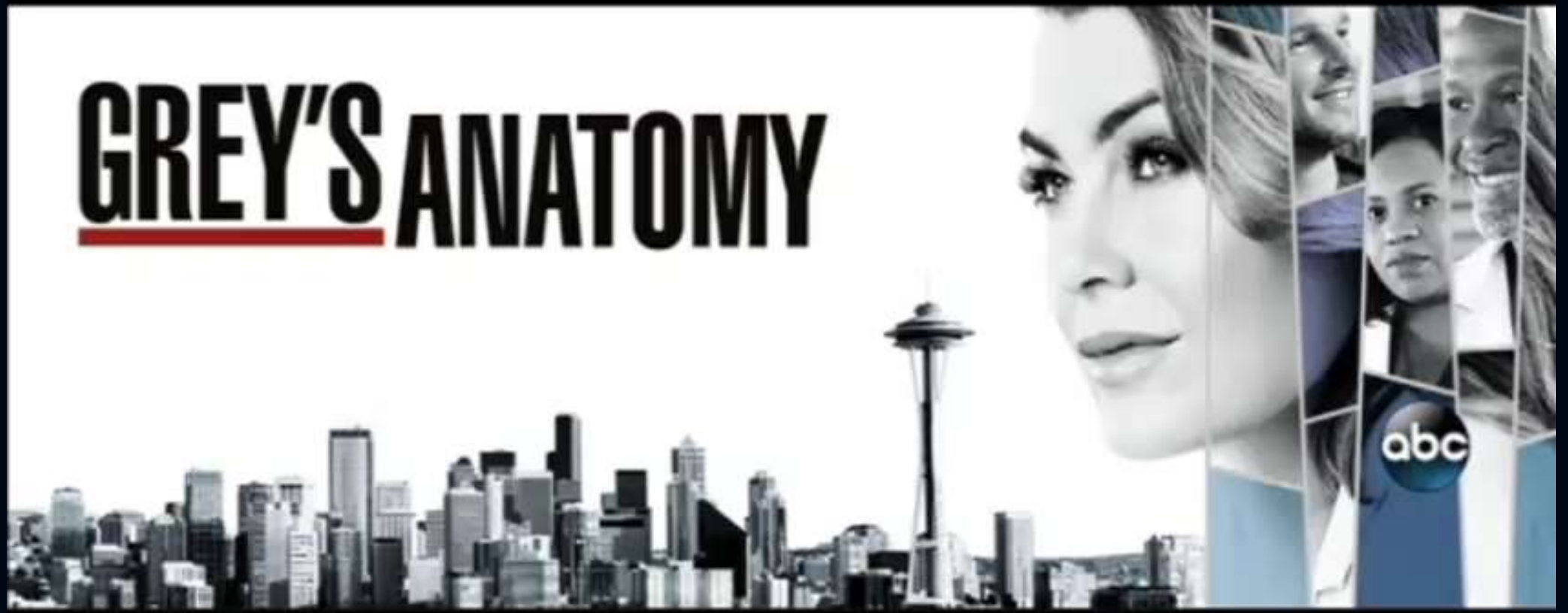
HIMSS NORTH CAROLINA Chapter

Agenda

- Hollywood's Hype
- The attack
- The impacts
- The recovery
- The cleanup
- The post mortem
- Lessons learned

Hollywood's Hype

HIMSS NORTH CAROLINA Chapter


GREY'S ANATOMY
abc

Prologue

HIMSS NORTH CAROLINA Chapter

Prologue

- The focus of this presentation will be the attack on one multi-hospital health system

however

- There will be a comparison of other attacks as well as estimates of impacts and predictions of future trends

Setup

- FirstHealth of the Carolinas is an integrated delivery network, based in Pinehurst, NC, and serving a 15 county region
  - Four hospitals (600 Beds)
  - 100 Ambulatory physician practices/locations
  - Implemented Epic enterprise-wide on 7/1/17
- Implemented several security tools
- Dedicated IT security staff consisting of:
  - CISO/Supervisor
  - Network Security – 3 Engineers/Analysts
  - Information Security - 3 Engineers/Analysts (includes Surveillance)

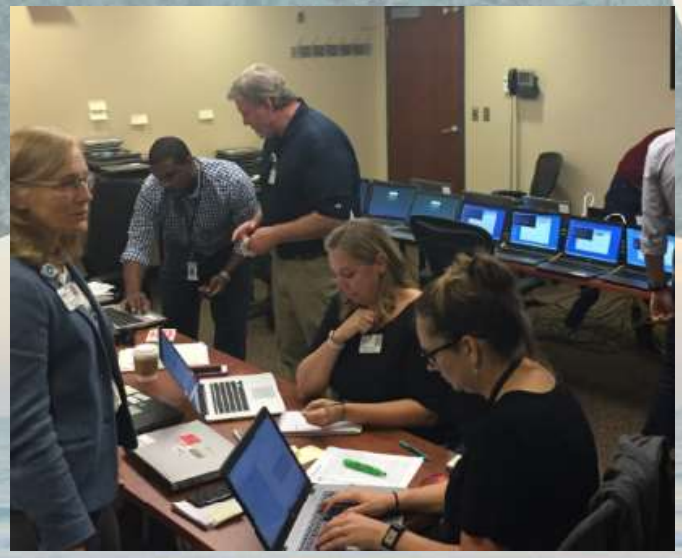
The Attack

HIMSS NORTH CAROLINA Chapter

The Attack

- The entry point - a user workstation
  - New variant of the WannaCry virus, coupled with the (NSA created) double pulsar virus
- The malware spread quickly, laterally, across the workstation environment
  - 10/17 at 12:30 pm – Received malware alert notifications
    - Network (FireEye and Cisco AMP)
    - End User (FireAmp and TrendMicro)
- Attack identified by SIEM and AV based on abnormal network traffic
  - Network connections to server farm and data farm were severed within 15 minutes
  - No automated quarantine possible - no “Zero Day” malware definition files
  - Not limited to traditional IT workstations
    - 30 PCs, 30 Laptops, over 1,000 thin clients, and *potentially* a few servers (approx. 1,100 devices)
- Data was never accessed, and “ransomware” never actually executed

The Response



The Response

- Communicated with Administration, Network Vendor, AV vendor, Security Consultants, and the FBI
- Pulled team together to assess situation and begin to plan next steps
- Misjudged the scope – failed to initiate incident command center
- Realized magnitude – requested help from Vendors and Peer Organizations
- AV Vendor developed new definition file
- Meanwhile – over 100 locations put on total downtime – paper

The Response

- Developed plan to wipe all infected and *potentially* infected devices
- Developed plan to isolate/filter all network connections, individually
- Created teams working two 12-hour shifts to re-image devices, apply missing patches, add two AV solutions, test, scan, monitor, and re-establish full network access (device by device)
  - Communications issues – misunderstandings, inaccurate maps, changes in approach/process – caused a *lot* of rework
  - Insufficient large capacity USB (thumb) drives
  - Temporary “admin” ID/PW to other staff
  - Night shift prepared maps and documentation/lists for day shift staff

The Impact

HIMSS NORTH CAROLINA Chapter

Impact on Operations

- Two full weeks of downtime – enterprise-wide
- Opened Incident Command Center – 24/7
- Paper processing for nearly *everything*
- Younger staff was often clueless – *"Thank God for older nurses!"*
- Needed many "runners" to go everywhere (pick up lab orders, etc.)
- Confusion and inconsistency re: backloading of data/charges
- "Downtime Boxes" were designed for 2-3 days
  - Ran out of forms and prescription pads
  - Used print shop for what we could
  - Old versions of paper order sets

Impact on Operations

- Phones initially impacted (on the same network)
  - Lost ACD/Menu functionality for several days
- OR Schedule reviewed for “elective” or “postpone-able” procedures
  - No PACS availability – Access to images a challenge
- BCA Devices – lost nearly all value after a couple of days
- IT had to focus on Payroll and Materials Mgt
  - You have to pay your staff and order your supplies
- EMR was never actually infected – but limited workstation access made it virtually unusable
  - Focused on a few workstations in order to maintain up to date census

Impact on IT

- Staff burn-out, mistakes, stress, irritability
- Forced a few “stay home” days for some staff
- Stress/Worry that any negative patient outcome would be our fault
- Stress/Worry about missing something critical
  - Access to servers/databases with critical cancer regimen data
  - Access to old clinical data/images
  - Access to allergy data, etc.
- “Remediation Services” not what was expected
  - Required obtaining extra staff from peer organizations and temp agencies

The Recovery

HIMSS NORTH CAROLINA Chapter

The Recovery

- 14 *days* of paper orders, charges, results, etc.
- 4+ *months* of matching patients with orders, charges, and results in the system
- Additional expense of $250K - $500K (overtime, special services, remediation assistance) not counting new security hardware or software
- No claims processing for 60+ days – No incoming cash flow
- Revenue reduction (lost revenue) of $2 million
- No progress on IT projects for several months

The Cleanup

HIMSS NORTH CAROLINA Chapter

The Cleanup

- Took a solid four months of enterprise-wide effort, but…
- It is *still* happening six months post event
- Confusion and inconsistency of cleanup process
  - Some departments and clinics entered their own backload of data
  - Others had ancillary departments enter their orders/charges
  - Still a few others did nothing, causing frustration and delays
    - *"Lab gets the revenue, they should do the work"*
    - *"Who has the paperwork now?"*
    - *"Our staff doesn't want the extra overtime or weekend work"*
    - *"We didn't cause this, why should we have to fix it?"*
- We still occasionally find a missing charge, order, or result

The Post Mortem

HIMSS NORTH CAROLINA Chapter

The Post Mortem

- Some devices deployed in a rush for “go-live” bypassed key work flow processes (some missed AV install or critical patches)
- A few servers were not fully patched (some unable to be patched, some scheduled, but not completed prior to the attack)
- Flaw in Microsoft SCCM
  - Just because you push out a patch doesn’t mean it processed successfully
  - We now do routine scans to ensure all patches are in place
- Old, un-patchable systems removed from the network
- IT Security likely understaffed, and needs more tools

The Post POST Mortem

- Need to plan for more network (micro) segmentation
- Need to move telecom to a separate network
- Need to do more active scanning
- Need for more security training (IT and all Staff)
- Need to investigate segmenting imaging
- Need to improve overall change management processes
- Need to open command center within 24 hours of incident

The POST POST Mortem

- Need to reconsider “downtime” box contents, plan for longer outage
- Need to test all BCA devices and off-line printing capabilities
- Need to add more BCA devices, and downtime computer workstations
- Leadership, Department, and Physician contact lists were a) out of date, and b) hard to find (when network is down)
- Need to quickly establish mini-registration/census location(s) and distribute information often
- Need better access to standardized forms
- Need better access to paper-based order sets
- Need a formal plan for who will do what (backloading of orders, charges, results) and other scanning

Lessons Learned

HIMSS NORTH CAROLINA Chapter

Comparing Other Ransomware Events

- WHO?
  - Small 200 bed hospital & Cloud hosted EHR
- OUTCOME?
  - Correlation between attack success & security maturity
- LESSONS LEARNED
  - The “minimum” level of security is never good enough
  - The threats are constantly improving – so should controls

The Problem Is Not Going Away

- Cost of cybercrime is expected to be $6 trillion by 2021 – more profitable than the world's drug trade. Cybersecurity Ventures, 2017 Annual Cybercrime Report.
- The average number of new ransomware variants detected per month is more than 30,000 – a number that is increasing.
  Internet Security Threat Report (ISTR), Dick O'Brien, July 2017
- Healthcare was the top industry hit by ransomware in 2017, with 45% of total cross-industry incidents. Beazley, 2018 Breach Briefing

Performing a Root Cause Analysis (RCA)

- Perform a RCA to determine why the event occurred
  - Use the opportunity to conduct a thorough gap assessment and update the risk analysis
- Develop an action plan to remediate all risks, especially closing the gaps that allowed the event to happen
  - Bad example: Colorado DOT https://www.denverpost.com/2018/03/01/cdot-samsam-ransomware-attack/
- Rule of Thumb: If the RCA doesn't end by documenting a management action, you are not done digging

Post Recovery: HIPAA Required Actions

- 45 CFR §164.308(a)(1)(ii)(D) *Information system activity review* (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports

- 45 CFR §164.308(a)(6)(ii) *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

LoProCo

- If you determine the Ransomware is not a reportable breach, you must document the LoProCo and keep it for six years.
  - It was a key document requested by OCR during their audits
- Key elements of the HIPAA Breach Analysis
  - Thorough discussion of the event, then:
    - The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re- identification;
    - The unauthorized person who used the protected health information or to whom the disclosure was made;
    - Whether the protected health information was actually acquired or viewed; and,
    - The extent to which the risk to the protected health information has been mitigated.
  - Recommendation based on the evidence.

The Adverse Impacts Last A Long Time

- The financial recovery following a ransomware event takes a minimum of six months, and even then, the unrecoverable costs are measurable in the millions. *A Ransomware Post Mortem*, Clyde Hewitt, Health Management Technology, March-April 2018
- 25% of patients have changed their provider following a data breach Accenture, 2017 Consumer Survey on Cybersecurity and Digital Trust.
- U.S. organizations that paid the ransoms were targeted and attacked again with ransomware 73 percent of the time. Business Wire March 27, 2018
- Forty five percent of U.S. companies hit with a ransomware attack last year paid at least one ransom; but only 26 percent of these companies had their files unlocked. Business Wire March 27, 2018

Action Plan

1. Perform a comprehensive gap assessment & risk analysis
2. Implement a security management policy
3. Remediate the highest risk
4. GoTo Step 1

We Are Not Good At Managing Security

- “More people are killed every year by pigs than by sharks, which shows you how good we are at evaluating risk.”

  Schneier, Bruce. Interview with Doug Kaye. IT Conversations: Bruce Scheier. 2004-04-16.


Thank you!
Dave Dillehunt
Vice President & CIO
FirstHealth of the Carolinas
Clyde Hewitt
Vice President, Security Strategy
CynergisTek
HIMSS
NORTH CAROLINA Chapter