Cyber Security and Ransomware:

Planning for Not IF, but WHEN it will happen

Jeffrey A. Tiesi, FACHE
Executive Vice President
SVP & COO

Ed Tangredi, CEM
Director of
Emergency Management

Today's Agenda

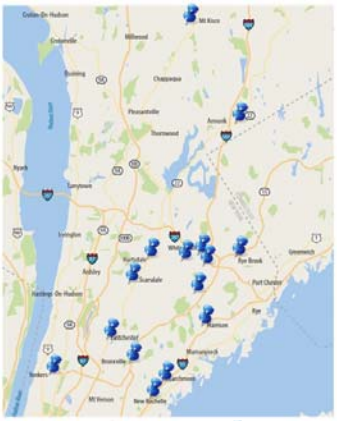
- A brief history of cyber attacks in healthcare
- Ransomware 101
- HIPPA and Joint Commission Standards
- Mitigation – Risk Assessment
- Preparedness Efforts
- Cyber Attack at White Plains Hospital
- Our Response
- Recovery and Next Steps

Emergency Management Cycle

White Plains Hospital at a Glance…

2016 Statistics:

- 292 Beds
- 18,174 Inpatient Discharges
- 1,900 Births
- 59,560 ER Visits
- 16,363 Surgical Procedures
- 40,052 Cardiology Procedures
- 212,120 Radiology Procedures
- 1,866,333 Lab tests
- 18 Off-site Practices
- ~ 1000 Members of medical staff



WPHPA Site

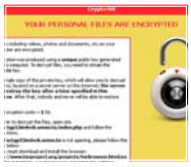
White Plains Hospital locations:

- Business Park Drive — Armonk
- Pondfield Road — Bronxville
- White Plains Road — Eastchester
- Mamaroneck Ave — Harrison
- Central Avenue — Hartsdale
- Boston Post Road — Larchmont
- Kisco Avenue — Mt Kisco
- North Avenue — New Rochelle
- S. Ridge Street — Rye Brook
- White Plains Road — Scarsdale
- Davis Ave — White Plains
- Longview Avenue — White Plains
- Greenridge Avenue — White Plains
- Maple Avenue — White Plains
- North Street — White Plains
- Westchester Avenue — White Plains
- Westchester Avenue — West Harrison
- Palmer Road — Yonkers

Ransomware 101

- Ransomware is a type of malware (malicious + software) that encrypts a victim's files, locking users out of the infected device/system or blocking access to encrypted files.
- In order to acquire the key to decrypt these files, the victim must pay a ransom, often in the form of bitcoin or other electronic currency.

Evolution of an Attack

(1) source	(2) infection	(3) ransom notice	(4) pay or ???
			
• Ransomware typically sent as an email attachment or an embedded code / link in a webpage or email • Emails historically generic (phising); increasingly targeted to specific individual (spear phising)	• Once opened or clicked, ransomware begins encrypting all available files, without user interaction or notification • If user's machine is connected, available files can include files on network, cloud, shared services, etc.	• Once encryption is complete, ransomware alerts the user of infection, blocks access to system / files and provides payment instructions for decryption key	• Key choice: – Pay ransom; or – Restore from backup

Ransomware Is easy

- Cybercriminals don't need to be "high-tech" or particularly tech savvy. All of the tools they require are available at reasonable cost.[1]
- "Ransomware-as-a-Service" is readily available and cheap and in some instances for free.[2]
- A phishing page and a mass spam email to deliver the Ransomware can be purchased in an off-the-shelf malware for about $150.[1]


THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate

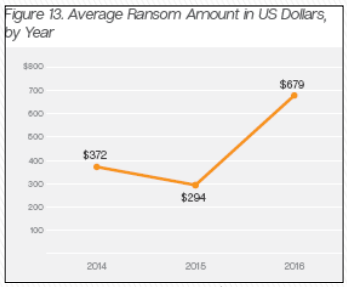
RISK & COMPLIANCE JOURNAL.

Ransomware Is Booming and Companies Are Paying Up

1. Kasperky, *Cybercrime, Inc.: how profitable is the business?, Dec. 2, 2014, https://business.kaspersky.com/cybercrime-inc-how-profitable-is-the-business/2930/.*
2. McAfee Labs, *Meet 'Tox': Ransomware for the Rest of Us*, May 23, 2015, https://securingtomorrow.mcafee.com/mcafee-labs/meet-tox-ransomware-for-the-rest-of-us/.

Ransomware Is Profitable

- Established business case for Ransomware
  - Ransomware will net criminals $1B (est.) in 2016.1
  - High-end Ransomware costs about $2k through dark net forums2; the average ransom demand is $6793.
  - An attacker needs to ransom four "normal" (individual) users (or one hospital / enterprise with mission-critical data) to generate a profit.



Source: Symantec, *Ransomware and Businesses 2016.*

1. David Fitzpatrick and Drew Griffin, *Cyber-extortion losses skyrocket, says FBI*, CNN.com, Oct. 5, 2016, http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/.
2. Institute for Critical Infrastructure Technology, *ICIT Ransomware Report: 2016 Will Be the Year Ransomware Holds America Hostage.*
3. Symantec Corporation, *Ransomware and Businesses 2016*, May 2016.

Hackers Love Healthcare

Healthcare is Big and Vulnerable

Giant Industry	• 5,627 U.S. Hospitals (AHA 2016 Report) • 35M hospital admissions per year + >100M outpatient encounters at doctor offices, hospital outpatient departments, pharmacies, behavioral health centers, etc. → innumerable patient records and data • Healthcare records are 10 times more valuable on the black market than credit cards

Technology Dependent	• Digital Health Records
	  • 90% of hospitals implemented EHR
	  • Health Information Exchange driving further digitization and connectedness
	• Delivery of care requires sophisticated technology (diagnostics, bedside point of care systems, etc.)
	• Wellness and prevention efforts technology dependent (distance care, wearables, implanted devices)

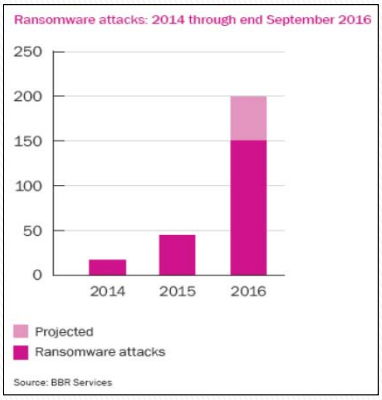
Hackers Love Healthcare

Healthcare is Big and Vulnerable

Rapid Change and Consolidation	• Unprecedented industry consolidation • Complex networks (patchworks) of "legacy" systems • Provide a collaborative, transparent, and real-time platform to deliver service regardless of where the expertise may lie
High Touch	• Staff intensive (most of whom have access to EHR and financial systems) • Staff splitting time between facilities requires access across multiple systems • Many non-employees permitted access (e.g., medical staff)
Immature Cybersecurity	• Outdated approaches, frequently failing at securing organizations from today's increasingly sophisticated cybercriminals • 2 major IT security issues: HIPAA-centric focus (defending patient records) and security measures defending against yesterday's issues

Healthcare Ransomware trends

- According to the FBI, Ransomware has quickly become one of the **larger threats** to healthcare cyber security.[1]
- At least **16 hospitals** have been attacked by **ransomware in 2016**.[2]
- Healthcare data breaches are frequent and impact everyone:
  - Nearly **90%** of hospitals reported a data breach in the past 2 years; **45%** had 6 or more data breaches.[3]
  - About **47%** of US population has had their personal healthcare data compromised over last 12 months.[3]



1. FBI, *Incidents of Ransomware on the Rise*, April 29, 2016, https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise.
2. Jessica Davis, *Ransomware: See the 14 hospitals attacked so far in 2016*, Healthcare IT News, Oct. 5, 2016, http://www.healthcareitnews.com/slideshow/ransomware-see-hospitals-hit-2016?page=1.
3. Institute for Critical Infrastructure Technology, Hacking Healthcare IT in 2016, January 2016.

Why is Healthcare a Target for Ransomware

"*Hospitals are the perfect mark for this kind of extortion. [They] are more likely to pay a ransom rather than risk delays that could result in death and lawsuits.*"[1]

- Staggering amounts of valuable electronic data, which is not required to be encrypted "at rest".
- Reliant on technology to deliver patient care.
- Increasing connectivity of care and interconnectivity of healthcare industry.
- Tremendous number of access points for criminals (systems and users).
- Insecure and antiquated networks vulnerable to attacks.[2]

"*It's very common for hospitals to have a large number of outdated and vulnerable systems on the network.*"

1. Kim Zetter, *Why Hospitals Are the Perfect Targets for Ransomware*, Wired.com, March 30, 2016.
2. Institute for Critical Infrastructure Technology, *Hacking Healthcare IT in 2016*, January 2016.

What's at Stake

- **Patient Health & Safety**
  - Loss of EMR access can impede the ability to treat patients.
  - Lack of control over essential medical equipment can endanger patients.
- **Regulatory Compliance**
  - Ransomware (or any malware) on a covered entity's or business associate's systems is a HIPAA security incident.[1]
  - Ransomware attack involving protected health information is presumptively a HIPAA Breach.[1]
  - State data security and breach reporting laws may also be implicated.

1. U.S. Department of Health and Human Services Office for Civil Rights, *Fact Sheet: Ransomware and HIPAA*, July 11, 2016.

What's at stake

- **Financial Implications**
  - Ransom payment
  - Business Interruption and Extra Expense
  - Incident response, legal, forensic IT, etc. expenses
  - Data restoration costs
  - Regulatory expenses – defense & fines (e.g., DHHS fines for HIPAA violations and associated defense costs)
  - Patient lawsuits
  - Notification expenses

*"The potential for corporate losses from cyber attacks goes far beyond downtime and lost revenue… If attacks delay the release of medicines to patients[, render inoperable or accessible EHR systems, or shut down critical medical equipment, they can endanger lives and result in **punitive damages**."*
Fiona Barry – Ex-Homeland Security Cyber Chief

What's at stake

- **Reputational Risk**
  - "*The reputational hit [from a breach]…* could be an ***extinction- level event***." Vincent Polley – Co-Author of American Bar Association Cyber-Security Handbook

The 5 Most Visible Cyber Attacks on Hospitals

Stolen Financial Data

Notable Example: Anthem

The first category of visible attacks on hospitals in the United States is stolen financial data. In 2015, hackers accessed personal information for 80 million customers and employees and stole tens of millions of records. It was recorded as one of largest data breaches of healthcare information discovered in history.

Insurance Fraud

Notable Example: Community Health Systems

The second category of visible attacks on hospitals in the US comes from cyber-criminals targeting personal data in order to participate in insurance fraud. Patient data like diagnosis codes, billing information, policy numbers, and birth dates is all that is necessary to file fake claims with an insurer, resulting in reimbursement for services never provided. It may also be used to make false IDs that can be used to buy illegal drugs for personal use or medical equipment that will be resold.

Ransomware

Notable Example: Presbyterian Medical Center

One of the more common types of attack occurring in 2016 has been ransomware. When this occurs, a hacker infiltrates the network and accesses data. It is then copied over and encrypted. Once encryption is complete, the original data will be deleted and data will be inaccessible until a ransom is paid. This usually results in an inability to access the EHR while the application is locked down; any communication has to be completed via telephone calls or faxes, resulting in an overall delay in patient care.

Social Engineering

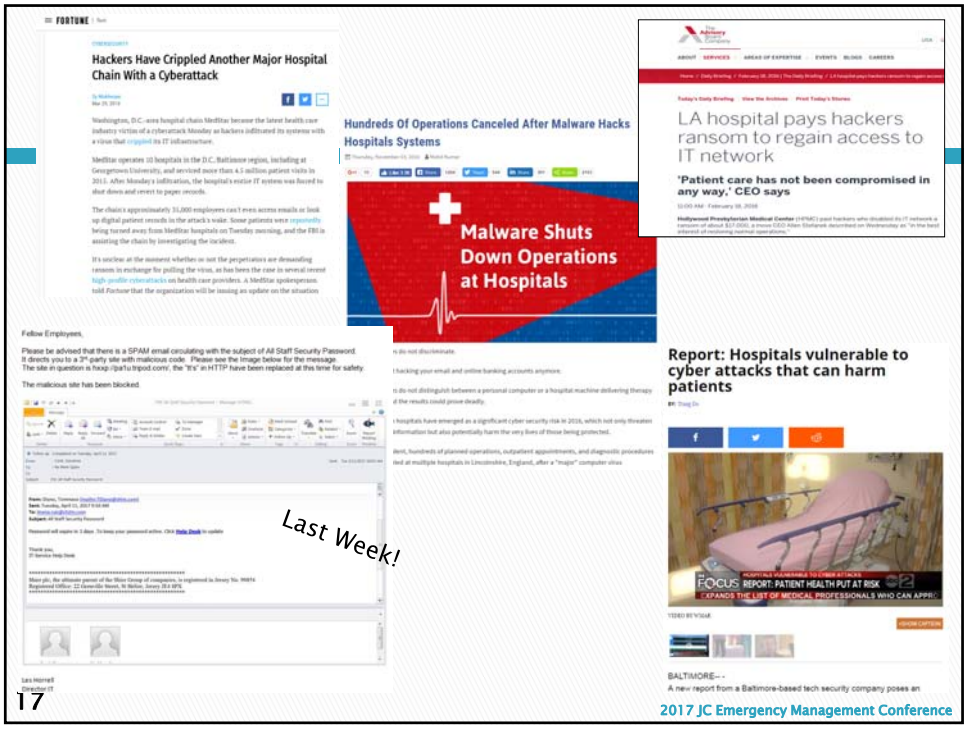
Notable Example: University of Washington Medicine

Social engineering has become a common method of deploying malware to infect systems. Hackers target companies that publically display their employees' contact information. Individuals are then sent phishing emails containing links or attachments that appear to be innocent in nature. But, when the link is accessed, it will immediately infect the users' computers and begin to spread throughout the rest of the health system.

MEDJACK

Notable Example: UCLA Health

MEDJACK is one of the latest methods of accessing a health system's network. This method will target medical devices that integrate with applications, often through methods that are not highly protected against. This allows backdoors to be created across an enterprise system, giving access to cyber-criminals for months before detected. Since it appears that nothing abnormal is occurring, data can be easily stolen.



JC EM Standards

- **EM.01.01.01, Element of Performance (EP) 6**: The hospital uses its hazard vulnerability analysis as a basis for defining the preparedness activities that will organize and mobilize essential resources.
- **EM.02.01.01, EP 4**: The hospital develops and maintains a written Emergency Operations Plan that describes the recovery strategies and actions designed to help restore the systems that are critical to providing care, treatment, and services after an emergency.
- **EM.02.02.01, EP 14**: The hospital establishes backup systems and technologies for the communication activities identified in the emergency management plan.

JC EM Standards (CONTINUED)

- **EM.02.02.11, EP 8**: The Emergency Operations Plan describes how the hospital will document and track patients' clinical information during emergencies.
- **EM.03.01.03, EP 14**: The evaluation of all emergency response exercises and all responses to actual emergencies includes the identification of deficiencies and opportunities for improvement; this evaluation is documented.
- **EM.03.01.03, EP 15**: The deficiencies and opportunities for improvement, identified in the evaluation of all emergency response exercises and all responses to actual emergencies, are communicated to the improvement team responsible for monitoring environment of care issues and to senior hospital leadership.

JC IT Standards

- **IM.01.01.03, EP 1**: The hospital has a written plan for managing interruptions to its information processes—paper-based, electronic, or a mix of paper-based and electronic.
- **IM.01.01.03, EP 2**: The hospital's plan for managing interruptions to information processes addresses scheduled and unscheduled interruptions of electronic information systems.

JC IT Standards (CONTINUED)

- **IM.01.01.03, EP 3**: The hospital's plan for managing interruptions to information processes addresses training for staff and licensed independent practitioners on alternative procedures to follow when electronic information systems are unavailable.
- **IM.01.01.03, EP 4**: The hospital's plan for managing interruptions to information processes addresses backup of electronic information systems.

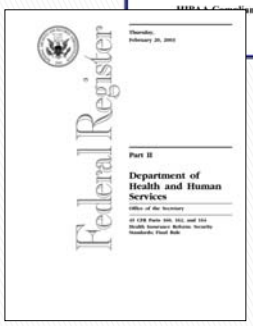
HIPPA Privacy and Security Rules

Electronic Protected Health Information

- The HIPAA **Privacy Rule** protects the privacy of individually identifiable health information, called protected health information (PHI), as explained in the Privacy Rule. The Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form. The Security Rule calls this information "electronic protected health information" (e-PHI).

HIPPA Privacy and Security Rules

- The HIPAA **Security Rule** requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. Specifically, covered entities must:
  - Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
  - Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  - Protect against reasonably anticipated, impermissible uses or disclosures; and
  - Ensure compliance by their workforce



Hazard Vulnerability Analysis

I don't see Cyber Attack!

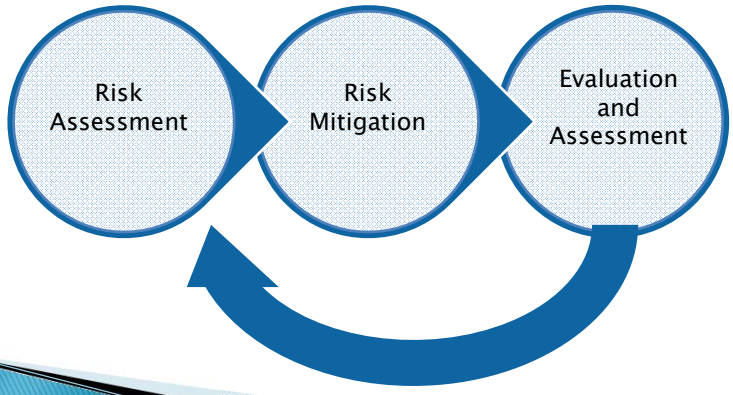
These values are categorized as follows:

321 to 400 HIGH HAZARD
241 to 320 MODERATELY HIGH HAZARD
161 to 240 MODERATELY LOW HAZARD
44 to 160 LOW HAZARD

The Group rated the 38 hazards as follows:

Hazard		Rating
SEVERE STORM – WINTER	* Previously Ranked at 222	285
MEDITECH FAILURE	* Previously Ranked at 273	269
TORNADO		263
HURRICANE	* Previously Ranked at 196	258
KENSICO DAM FAILURE	* Previously Ranked at 259	255
SEVERE STORM	* Previously Ranked at 257	246
TERRORISM – BIOLOGICAL		245
FIRE	* Previously Ranked at 260	242
BUILDING COLLAPSE		239
EXTREME HIGH TEMPATURES		239
TERRORISM – CHEMICAL		239
TERRORISM – RADIOLOGICAL		238
INDIAN POINT INCIDENT	* Previously Ranked at 250	236
FLOOD – EXTERNAL	* Previously Ranked at 252	231
EARTHQUAKE	* Previously Ranked at 202	229
ELECTRICAL POWER FAILURE – SUPPLIED		228
WORKPLACE VIOLENCE	* Previously Ranked at 230	225
MCI – TRAUMA		223
EPIDEMIC		216
BURN SURGE		208
MCI – CHEMICAL		206
IT SYSTEM TOTAL FAILURE		201
SURGE CAPACITY / HIGH CENSUS	* Previously Ranked at 222	198
BOMB THREAT		189
STEAM FAILURE		186
HVAC FAILURE		181
HAZMAT (IN TRANSIT)		180
RADIOLOGICAL SPILL – INTERIOR		180
ELECTR FAILURE - EMERG POWER	* Previously Ranked at 178	180
PANDEMIC		179
MEDICAL GAS FAILURE		175
CONSTRUCTION CRANE COLLAPSE	* Previously Ranked at 160	174
ELECTRICAL INFRAST FAILURE		160
BOIL WATER ALERT		158
LOSS OF WATER		158
INFANT ABDUCTION		136

Ongoing Risk Assessment & Mitigation Process



White Plains Hospital Cyber Security

- April 2015 – MML (Medical Management LLC) billing data breach affecting 20,000-30,000 patients in 8 states; potential breach of 1,177 patients at WPH emergency department. In the end, no WPH patients were affected.
- Fall 2015 – WPH partnered with ***Grey Castle*** to perform a Comprehensive IT security project
- February 22, 2016 – Report of GreyCastle Assessment to Board
- March 24, 2016 – Ransomware "Locky" virus attack at WPH. Successfully isolated with no significant business interruption
- October 24, 2016 – Update to Board… 9 of 10 GreyCastle recommendations implemented; 1 added to create an ongoing multi-year integrated security plan with System ISO (Information Security Office)

White Plains Hospital Cyber Security

- Comprehensive IT review that assessed security across three domains:
  1. HIPAA Risk Assessment – identify weaknesses in organizational security and deviations from HIPAA compliance requirements
  2. Penetration Testing – assess how security controls and protective measures would withstand a simulated real-world attack
  3. Vulnerability Assessment – purely technical assessment of how current security controls compare to industry standard best practice (e.g. patch management)

White Plains Hospital Cyber Security

- Summary findings…
  1. WPH is "average" to "above average" for similar organizations.
  2. It won't take much for WPH to go from "good" to "very good".
  3. We found nothing that was surprising or of immediate concern.
  4. WPH considers HIPAA compliance an important component of its business process and its HIPAA compliance program is of a mature state.

Cyber Security Assessment – 2016 Action Plan

GreyCastle Security Assessment -- actions list with priorities and timeline

Month	1	2	3	4	5	6	7	8	9	10
PRIORITY	Mar '16	Apr '16	May '16	Jun '16	Jul '16	Aug '16	Sep '16	Oct '16	Nov '16	Dec '16
HIGH --DELAYED	Create multi-year **security plan**			Delayed						
HIGH -- COMPLETE	Strengthen and monitor role based **"access control"** practices									
HIGH -- COMPLETE	Remove / clean-up old, **unsupported software**									
ONGOING (Phase 1 Complete)	Conduct Cyber-security / password awareness education on **"Social Engineering"** to reduce risk to phishing schemes									
HIGH -- UNDERWAY (Partially Complete)	Implement **2-factor authentication** for remote access									
HIGH -- COMPLETE	"Harden" physical penetration, such as **open network ports** in high-traffic areas									
HIGH -- COMPLETE	Develop/update routine process for **software patch updates** mgmt.									
HIGH -- COMPLETE	Develop/update **emergency mgmt. contingency** plan for access to inpatient electronic medical records									
HIGH -- COMPLETE		Develop/update policies & supporting procedures that **strengthen compliance with HIPAA**								
HIGH -- COMPLETE		Implement **audit / alert system** for security incidents								
MEDIUM -- UNDERWAY Part of security plan					Develop/update an on-going process for addressing system vulnerabilities					
MEDIUM -- UNDERWAY Part of security plan					Develop/update security guidelines for infrastructure config.					
COMPLETE	Setup process for reviewing BAA agreements									
MEDIUM -- UNDERWAY Part of security plan			Collaborate w Legal and Purchasing to assess supplier vulnerabilities							
LOWER PRIORITY						Establish and deploy metrics for measuring security prog.. effectiveness				
		Assess credit card payment standards								

Indicates ORIGINAL Timeline

Indicates ACTUAL Timeframe

Summary of Recommendations and Updates

- Role-based "access control" practices need bolstered and audited; updated protocols and processes; *(Completed in May)*
- Remove and clean up use of old unsupported software (e.g. Windows XP, Office and Java); *(Complete in April)*
- Conduct ongoing cyber security/ password awareness education on "Social Engineering" so employees do not fall prey to phishing schemes; *(Completed in October)*
- Implement "two factor" authentication for remote access; *(Incomplete)*
- Increase physical penetration hardening for open network ports in high traffic areas such as conference rooms; *(Completed in April)*

Summary of Recommendations and Updates (CONTINUED)

- Implement routine process for software updates and patch management; *(Completed in April)*
- Develop/update for Emergency Management Response Plan to include contingency plan for medical record access *(Completed in June)*
- Develop/update policies and procedures to strengthen HIPAA compliance program *(Completed in August)*
- Implement audit/alert system for cyber security incidents *(Completed in May)*

Summary of Recommendations and Updates

- Maintain an inventory of the Business Associate agreements, periodically review and update; conduct vendor risk assessments; *(Completed in June)*
- Create On-going Multi-year Security plan; *(Underway, ongoing)*

Summary of Results from GreyCastle Phishing Test

1. **Baseline Phishing Test → 6/3**
   - 80.8% pass rate
   - 9 Security Awareness Training Sessions held in June
2. **Baseline Phishing Test → 7/18**
   - 91.9% pass rate (11.1 point improvement following the first 9 training sessions)
   - 18 Security Awareness Training Sessions held in September and October
   - 100% of WPH employees had attended a Security Awareness Training Sessions by the end of October
3. **Post-training Phishing Test → 12/8**
   - 93.7% pass rate (1.8 point improvement following training sessions)
4. **Remediation**
   - Based on outcome of the December phishing test, additional training will be provided for employees that did not pass

March 24, 2016

Event Chronology and Response

- At 08:48 AM user "Y.zzzzzz" received an email that contained a Microsoft Excel attachment. This email appeared to come from "XXX"
- At 09:26 AM user "Y.zzzzzz" opened the attachment, which contained a malicious macro and other malware.
- At 09:59 AM the PC named "WDCDC04" was encrypted due to a variant of the "Locky" malware. All user files became immediately locked and inaccessible. User not aware at that time.
- At 10.16 AM a different user reported their files were locked; desk top deployed; PC isolated and unplugged from network; call to alert Dell, network scanning initiated; 5 additional PC's removed by WPH IT. – CRITICAL FIRST STEP
- At 12.00 PM Noon escalation to CIO; at approximately 1.00 PM Administrator-on-Call notified.

EOP Initial Task:

Office of Emergency HICS Management

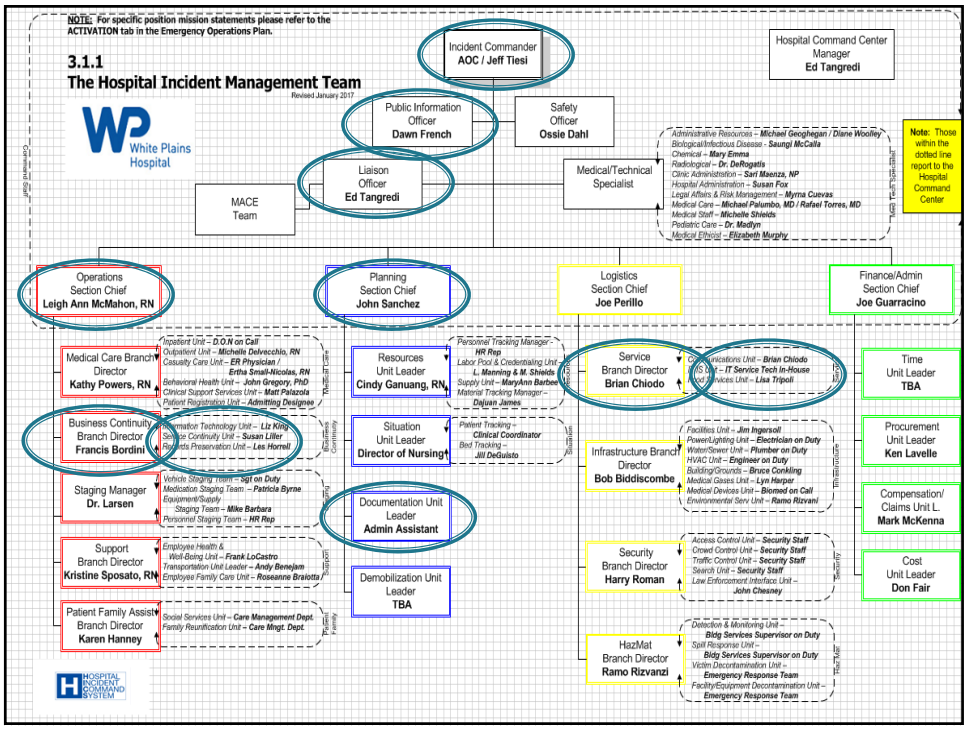
1.1 Initial Task List:

At the initial onset of an incident affecting normal hospital operations, remain calm and follow the task listed. This will get you through the initial response and the first 30 -60 minutes until other members of the Hospital Incident Management Team arrive.

- ☐ Rescue / evacuate anyone in immediate danger.
- ☐ Contact the Switchboard Operator and direct them to make the appropriate overhead announcement.
  - Code Red (Fire when the fire bells are inactive)
  - Code 5-0 (Security)
  - Code Pink (Infant or Child abduction)
  - Code Silver (Active Shooter)
  - Code HICS (emergencies not otherwise identified by code designation)
- ☐ Change the message on the HICS Hotline 2300 (see procedure on back of this page)
- ☐ Notify Switchboard to call and notify the Administrator on Call and the Primary Fan Call List of the initial incident.
- ☐ Assign a staff member to follow you and act as a scribe. Write down incident findings, actions taken and any other relevant notes.
- ☐ Establish a Command Post. This may be at the scene of the incident, ie; the Emergency Rm, or in the Administrative Conference Rm. (Hospital Command Center). This is where the Incident Management Team will report to initially.
- ☐ Assume duties as the Incident Commander & follow guidelines on the Incident Commander Job Action Sheet. Brief arriving Incident Management Team members.
- ☐ Transfer Command to the AOC or Executive Vice President when they arrive.

Event Chronology and Response

- At 1.35 PM, AOC on-site with CIO, initiate GreyCastle incident response; cyber techs deployed and in route to WPH; HICS called
- At 2.20 PM formal Incident Command established in HCC
- At 2.45 PM Jeff Tiesi, IC, brief Jack Wolf, Montefiore CIO; Jack and staff join incident command call underway
- Ongoing fact gathering, initial diagnosis and development of specific game plan as determined by GreyCastle, WPH and MIT
- At approximately 5.00 PM GreyCastle team arrive; initiate forensic analysis of affected "ground zero" PC
- Initial call continued until approximately 5.30 PM.
- Subsequent status update/ decision making calls occurred at 7.00 PM, 10.00PM and on Friday at 9.00 AM,11.45 PM and 2.30 PM ET when "all clear" was confirmed.



Recovery

Restoring Normal Operations & Terminating HICS:

- Communication to staff that normal operations have resumed
- Examination of Cyber Liability & Reporting Obligations
- Re-image of assets and deployment
- Staff education
  - Critical that 100% is achieved with Phishing test verification
- Ongoing awareness

Hotwash

How we Responded?

- We followed our IT protocols and used our emergency management systems **without hesitation**:
  - Formally activated Hospital Incident Command System (HICS)
  - Had previously engaged and established relationship with GreyCastle that lead to immediate deployment of the their emergency incident response team for digital forensics, analysis and cyber investigation.
  - In parallel we alerted Dell for e-mail quarantining, firewall and anti-virus response services
  - Early communication and coordination with System IT
  - Early an ongoing communication with managers and staff

Key Findings and Next Steps

- Immediate Incident Response – **Key Activities**:
  - Pursue immediate containment of the intrusion
  - Analyze log files, reports and other data to determine the origination and extent of the intrusion (forensics)
  - Ensure that no ePHI or PII was exfiltrated
- Immediate Incident Response – **Key Findings**:
  - (6) PC's affected; disconnected from network/ removed from service
  - Confirmation that no information of any sort was exfiltrated

Key Findings and Next Steps
(CONTINUED)

- Next Steps and Follow-up
  - Immediately take actions, if possible, to prevent future incidents of the same type; evaluating impact of implementing global restriction of macros
  - Restore PCs/resume normal operations as quickly as possible
  - Communicate to all staff the extent of the incident and the steps that they should take to assist
  - Continue to implementation our Cyber Security Assessment Action Plan

Staff Education

Pre-Incident Considerations

- **Assemble the Team**
  - Internal – RM, IT, Legal
  - External – Legal, PR, Broker/Insurer
- **Identify the Risk**
  - ERM Basics: What kind of data you have: How much? Where is it? Why do you have it? Who has it? Who gets to see it?
  - What vendors and other 3rd parties have access?
- **Elevate the Issue**
  - Board education and involvement is critical
- **Cyber Incident Response Plan**
  - Is it stale?
  - Outside expert review?
  - HIPAA Compliance

Pre-Incident Considerations

- **Business Continuity Plan**
- **Table Top Exercises (fire drills)**
- **Education, Education, Education**
- **Vendor Contracts / Issues**
  - Data security responsibility and requirements
  - Indemnity for breaches
  - Breach notification requirements
- **Insurance**
  - Funding mechanism; not a substitute for preventive measures and pre-loss planning
  - Does your coverage match your exposure?
  - Meet and use panel vendors before a loss
- **IT Cybersecurity**
  - Identifying who owns it and working to ensure this remains a priority.

Post-Incident Considerations

- **Assemble and Inform the Team**
  - Internal – RM, IT, Legal
  - External – Legal, PR, Broker/Insurer
- **Pull Cyber Incident Response Plan**
- **Notify cyber insurer(s)**
- **Isolate the infected equipment**
- **Data recovery / restoration**
- **Pay the ransom?**
- **Breach notification and HIPAA considerations**
  - Get qualified legal counsel involved immediately. Relatively short windows under some laws.
- **Post-Mortem / Remediation**

Resources

November 2016
Issue

US Computer Emergency Readiness Team:
www.us-cert.gov

FBI Internet Crime Complaint Center:
www.ic3.gov

Federal Trade Commission page on online security:
www.consumer.ftc.gov/topics/online-security

American Hospital Association cyber security portal:
www.aha.org/advocacy-issues/cybersecurity.shtml

US Centers for Medicare & Medicaid Services policy for information security and privacy: www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/IS_Policy-.pdf

Resources
(CONTINUED)

November 2016
Issue

US Food and Drug Administration page on medical devices and cyber security:
www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

National Institute of Standards and Technology's (NIST's) framework to reduce cyber risks to critical infrastructure:
www.nist.gov /programs-projects/cybersecurity -framework

Assistant Secretary of Preparedness and Response article on cyber security best practices for health care organizations:
www.jointcommission.org/assets /1/6/ASPR-TRACIE-Newsletter -The-Exchange-Cyberattack.pdf

The Joint Commission also has an online portal for emergency management with a special section on cyberattacks:

www.jointcommission.org/emergency_management_resources_cyber_attack)

Questions/Discussion

Thank you!

We may be contacted at:
etangredi@wphospital.org
914-681-2033

White Plains Hospital