CHITREC
CHICAGO HEALTH INFORMATION TECHNOLOGY REGIONAL EXTENSION CENTER

What You Need to Know about the MU Security Risk Analysis

November 8, 2017

Janet Baxter, MBA, RHIA
Eva Winckler, moderator

Agenda

Security Risk

Why do the Analysis

What’s in the Analysis

How to Do it

Where to Get Help

Why Analyze Risk

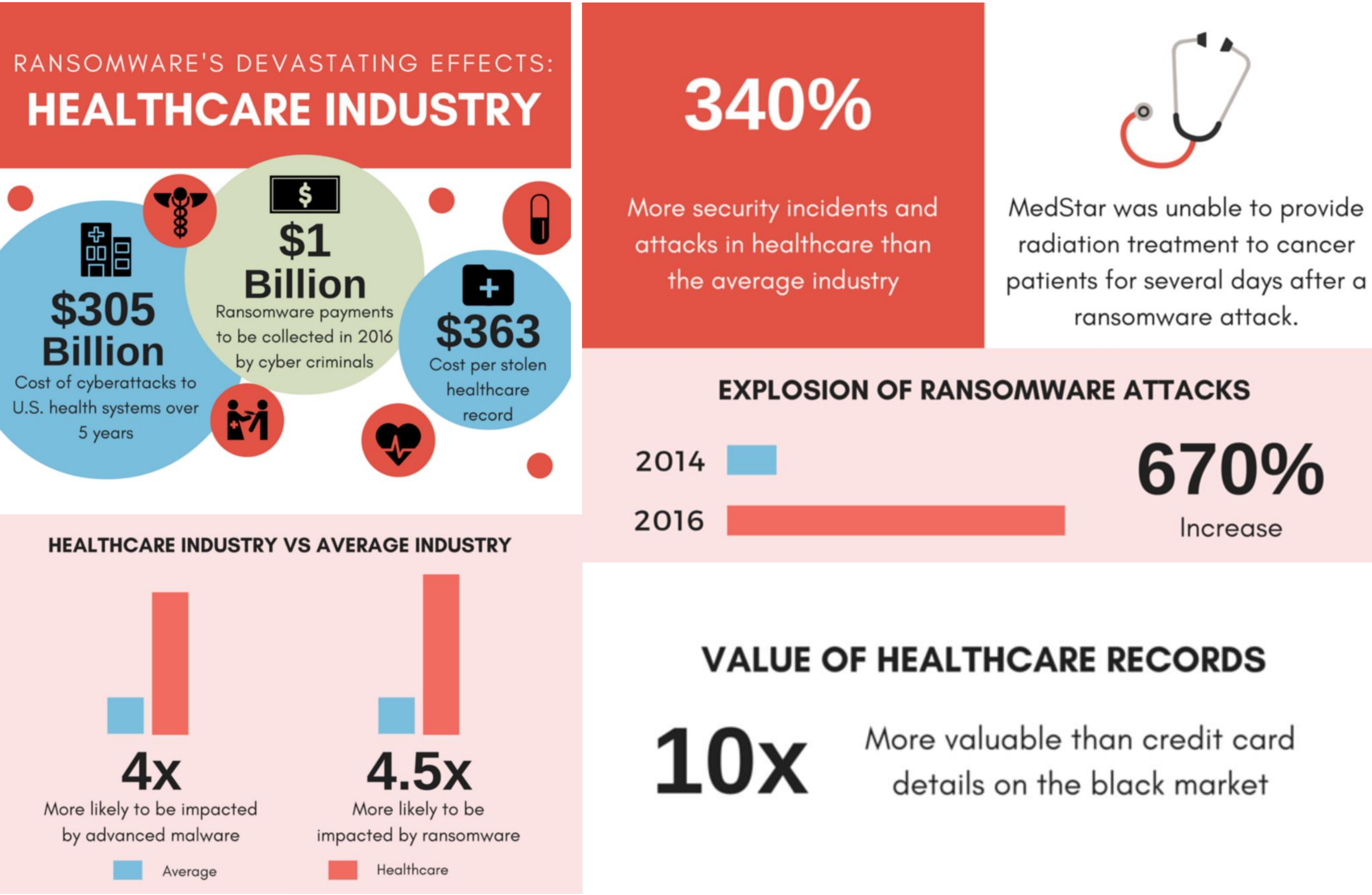
- To address all risks to electronic protected health information (ePHI)
  - Keep confidential
  - Keep accurate and available
- Certified EHRs have some security features, but you and your staff must use them and keep all PHI safe

Breach Happens

- Network server
- Email
- Desktop Computer
- Paper/ Film
- Laptop
- Mobile Devices
- Storms & Floods
- Burst pipe
- Fire
- Lost laptop
- Unlocked door
- Intentional breach

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

CHITREC



RANSOMWARE'S DEVASTATING EFFECTS:

HEALTHCARE INDUSTRY

$305 Billion
Cost of cyberattacks to U.S. health systems over 5 years

$1 Billion
Ransomware payments to be collected in 2016 by cyber criminals

$363
Cost per stolen healthcare record

340%
More security incidents and attacks in healthcare than the average industry

MedStar was unable to provide radiation treatment to cancer patients for several days after a ransomware attack.

EXPLOSION OF RANSOMWARE ATTACKS

670%
Increase

HEALTHCARE INDUSTRY VS AVERAGE INDUSTRY

4x
More likely to be impacted by advanced malware

4.5x
More likely to be impacted by ransomware

VALUE OF HEALTHCARE RECORDS

10x More valuable than credit card details on the black market

What is your plan for when this happens?

Analysis has Value

- Helps to plan in the event of a breach
- Maintain trust of patients and partners
- Business continuity
- Builds staff awareness
- Prevent breaches
  - Negative press
  - Patient dissatisfaction
  - Inadequate information for patient care

Security Risk Analysis is Required

- HIPAA
- Meaningful Use
- Advancing Care Information category of MIPS
- Sarbanes-Oxley Act
- Etc.

Meaningful Use Objective

- Protect electronic protected health information (ePHI) created or maintained by the CEHRT through the implementation of appropriate technical capabilities.
  - Must attest YES to:
    - conducting or reviewing a security risk analysis
    - implementing security updates as necessary
    - correcting identified security deficiencies
  - Maintain documentation in case of audit

Measure

- Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI created or maintained by CEHRT in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the EP's risk management process.

In other words

- You are documenting that you have explicitly considered all reasonable threats and done what you can to either
  - prevent that event
  - or to minimize damage from it
- The document allows easy communication of considerations and facilitates change to reduce risk

HIPAA Rules

- Privacy Rule
  - Who may have access to PHI

- Security Rule
  - Who is responsible for ensuring that only the right people have access to ePHI
    - Covered entities

Security Rule Requires

- Covered entities maintain safeguards for protecting ePHI.
  - reasonable and appropriate
  - administrative, technical, and physical
- Specifically, covered entities must:
  - Ensure confidentiality, integrity, and availability
  - Identify and protect against reasonably anticipated threats
  - Protect against reasonably anticipated, impermissible uses or disclosures
  - Ensure compliance by their workforce.

Security Risk Analysis

- Documented assessment
  - Risks to ePHI (reasonably aniticipated)
  - Assessment of impacts and possibilities
  - Mitigation activities
- Covers all technology
- Includes staff and business associates

Who is Responsible

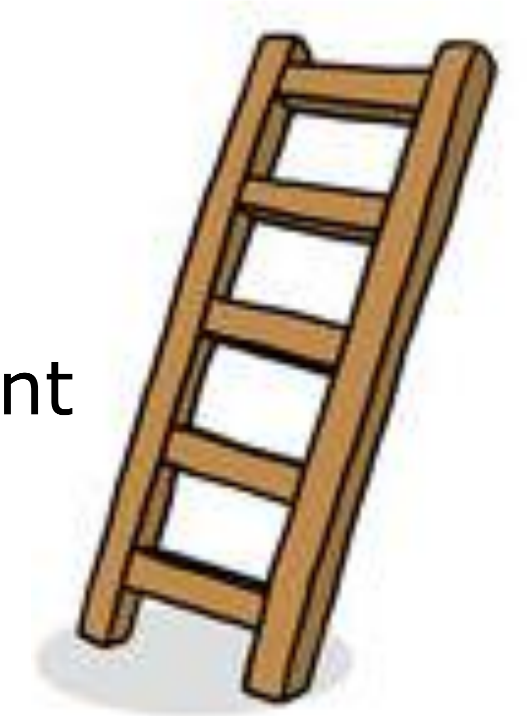
- Security Officer, Privacy Officer
- Initially, IT was responsible for assessing technology related risks
- Enterprise approach is wiser
  - Financial implications
  - Human resources, training, productivity
  - Senior decision makers decide the acceptable level of risk
  - Staff and patients
  - Interview to get wide risk experiences

How to Conduct the Analysis

- Office of Civil Rights (OCR) has issued guidance, but there is not one method
  - Flexible for large and small practices
  - Utilize the most effective safeguards
- You are not expected to eliminate all risks
  - Address what is reasonable
  - Continue to assess and make changes
- Must complete at least annually
  - New technology, upgrades

Steps to Success

1. Document Inventory
2. Determine Risks
3. Document the Impacts
4. Document Probabilities
5. Assess the Risks and Document
6. Address High Risks and Document



CHITREC

1. Document Inventory

- Business associates and information flows
- Assets – where is ePHI
  - EHR system
  - Practice Management/ Scheduling a or Billing
  - Document Management System/ scanner
  - Fax
  - Phone system/ voice mail
  - Copier or printer

2. What are the Risks

- Someone can compromise the confidentiality of your ePHI
- Someone might inappropriately alter or delete your ePHI, effecting its integrity
- Your ePHI might not be available when you need it

Sample Risks

- Natural disaster wipes out building
  - Or one part of your office
  - Or your data center
- Hacking, virus, ransomware
- Disgruntled employee wants revenge
- Information being exchanged is sent to the wrong recipient
- Information lost or left in a public place (mobile devices)

3. Document Impact of each Risk

- Overall harm or loss that could occur
- Use the scale that is most appropriate for your practice
- When it happens, what is the result?
  - The information can be lost or changed
  - The wrong person can access the information
  - The information is not available timely to the right people

4. Document the Likelihood of each Risk

- Is it going to happen?
  - Geographic, historical information
  - More users leads to higher risk
- Use a scale that is appropriate for your practice

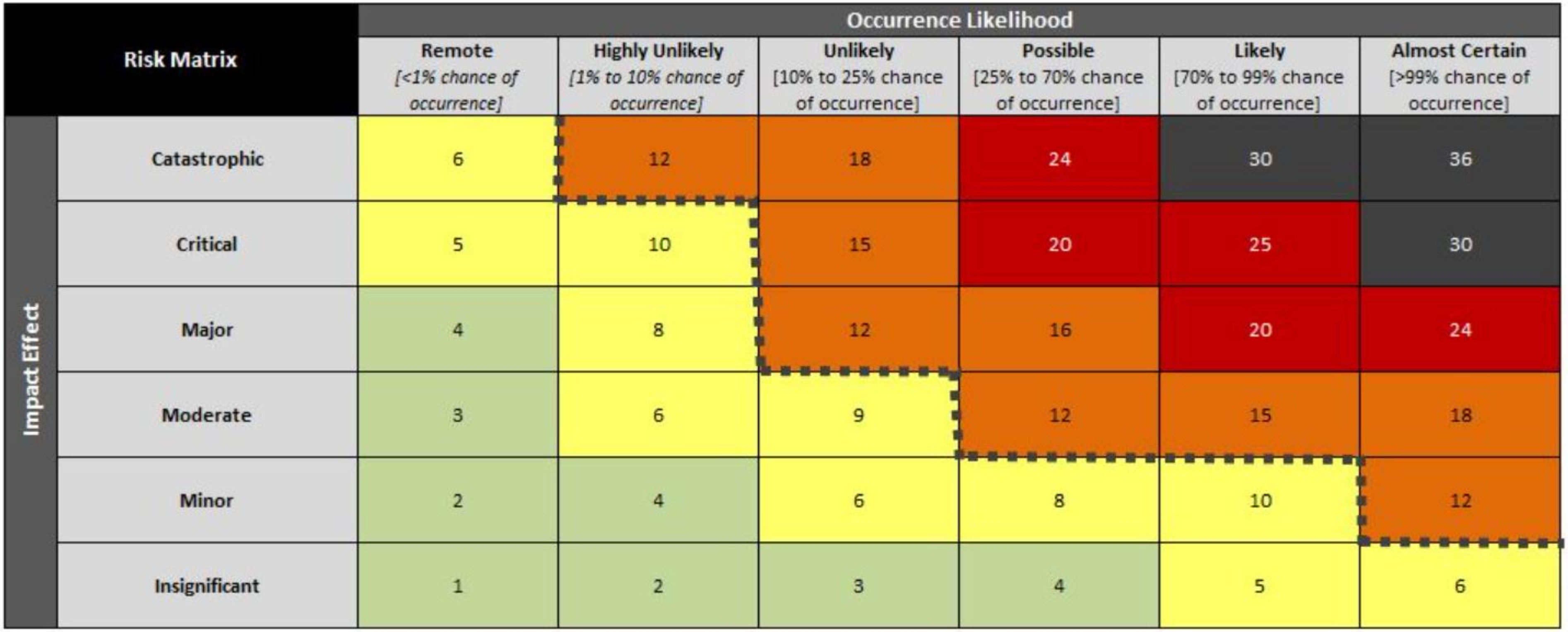
5. Assign Risk Scores

- Assess each risk for likelihood and impact
- Select appropriate scale
  - Enough levels to assess risk
  - Not more than you need

Simple Risk Matrix

	Low Probability	Medium Probability	High Probability
Low Impact	Low Risk	Low Risk	Low Risk
Medium Impact	Low Risk	Medium Risk	Medium Risk
High Impact	Low Risk	Medium Risk	High Risk

Sample Risk Matrix



Risk Matrix		Occurrence Likelihood					
		Remote *[<1% chance of occurrence]*	Highly Unlikely *[1% to 10% chance of occurrence]*	Unlikely [10% to 25% chance of occurrence]	Possible [25% to 70% chance of occurrence]	Likely [70% to 99% chance of occurrence]	Almost Certain [>99% chance of occurrence]
Impact Effect	Catastrophic	6	12	18	24	30	36
	Critical	5	10	15	20	25	30
	Major	4	8	12	16	20	24
	Moderate	3	6	9	12	15	18
	Minor	2	4	6	8	10	12
	Insignificant	1	2	3	4	5	6

Source: complianceforge.com

CHITREC

6. Address Risks and Document

- Address risk and document what you are doing or have done
- For risks you choose not to address, document why
  - Cost
  - Availability of technical resources
  - Something is expected to change
    - New location
    - New system
    - Etc.

Learn during the Process

- Discuss and share ideas, findings
- Aim for consensus on risk scores
- Recognize that there are some risks you cannot eliminate
- Train and share with staff

Repeat

- The Security Risk Analysis is the first step in a complete Security Management Process
  - Guard against and react to security incidents
    - Administrative Safeguards
    - Physical Safeguards
    - Technical Safeguards
- Update the Analysis at least annually
- Repeat with upgrades or installation of new technologies

Security Risk Assessment Tool

- Lots of information about HIPAA and other requirements, FAQs and more
- Small or Medium Size Practice
- Step by step guide. Suggests threats and safeguards
- https://www.healthit.gov/providers-professionals/ehr-privacy-security

Free

Identify
Assess
Manage
Safeguard

Where to Get Help- Free

- CMS and OCR Tip Sheet
  - https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/2016_SecurityRiskAnalysis.pdf
- Specifications for Meaningful Use
  - https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/MedicaidEPStage2_Obj1.pdf

More Help*

- Many consultants are available
  - Look for one that specifically offers Security Risk Analysis for meeting your requirements
  - Call the MU Help Desk for list of consultants that have attended training with CHITREC
- Templates are available on line
- Automated SRA guides or programs

* The Meaningful Use Help Desk and CHITREC do not endorse any consultants or products. These are listed to provide a starting point for practices that choose to engage outside help

Check Online

- Security Risk Analysis
- Security Risk Assessment
- HIPAA
- NIST

Scroll for many options! Some are ads

The Meaningful Use Help Desk and CHITREC do not endorse any consultants or products. These are listed to provide a starting point for practices that choose to engage outside help

This is just the beginning

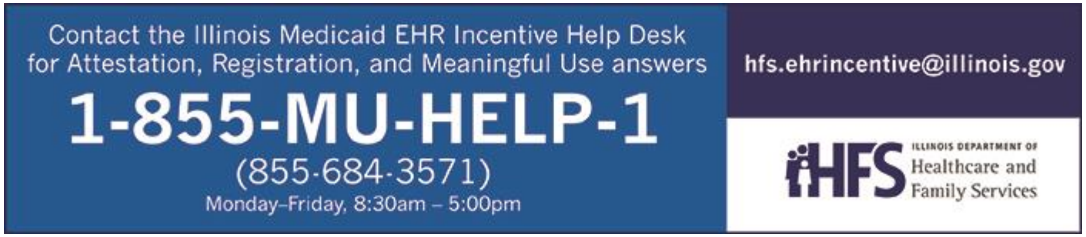
Today we have briefly covered

- Why do the Analysis
- What’s in the Analysis
- How to Do it
- Where to Get Help

Security Management is a process

Ongoing, repeat the analysis as needed

Questions?



Contact the Illinois Medicaid EHR Incentive Help Desk
for Attestation, Registration, and Meaningful Use answers

1-855-MU-HELP-1

(855-684-3571)

Monday–Friday, 8:30am – 5:00pm

hfs.ehrincentive@illinois.gov

HFS ILLINOIS DEPARTMENT OF
Healthcare and
Family Services