HIPAAtrek

Guiding Your HIPAA Compliance

Incident Response Workshop

Presented by Sarah Badahman
sarah@hipaatrek.com
314-272-2600

Security in Healthcare

We are the Weakest Link

- 320% increase in healthcare attacks 2015 to 2016
- Hackers exploit the fact that healthcare professionals are nurturers and caregivers by nature
- Technology has grown faster than security measures

Patient Data on the Black Market

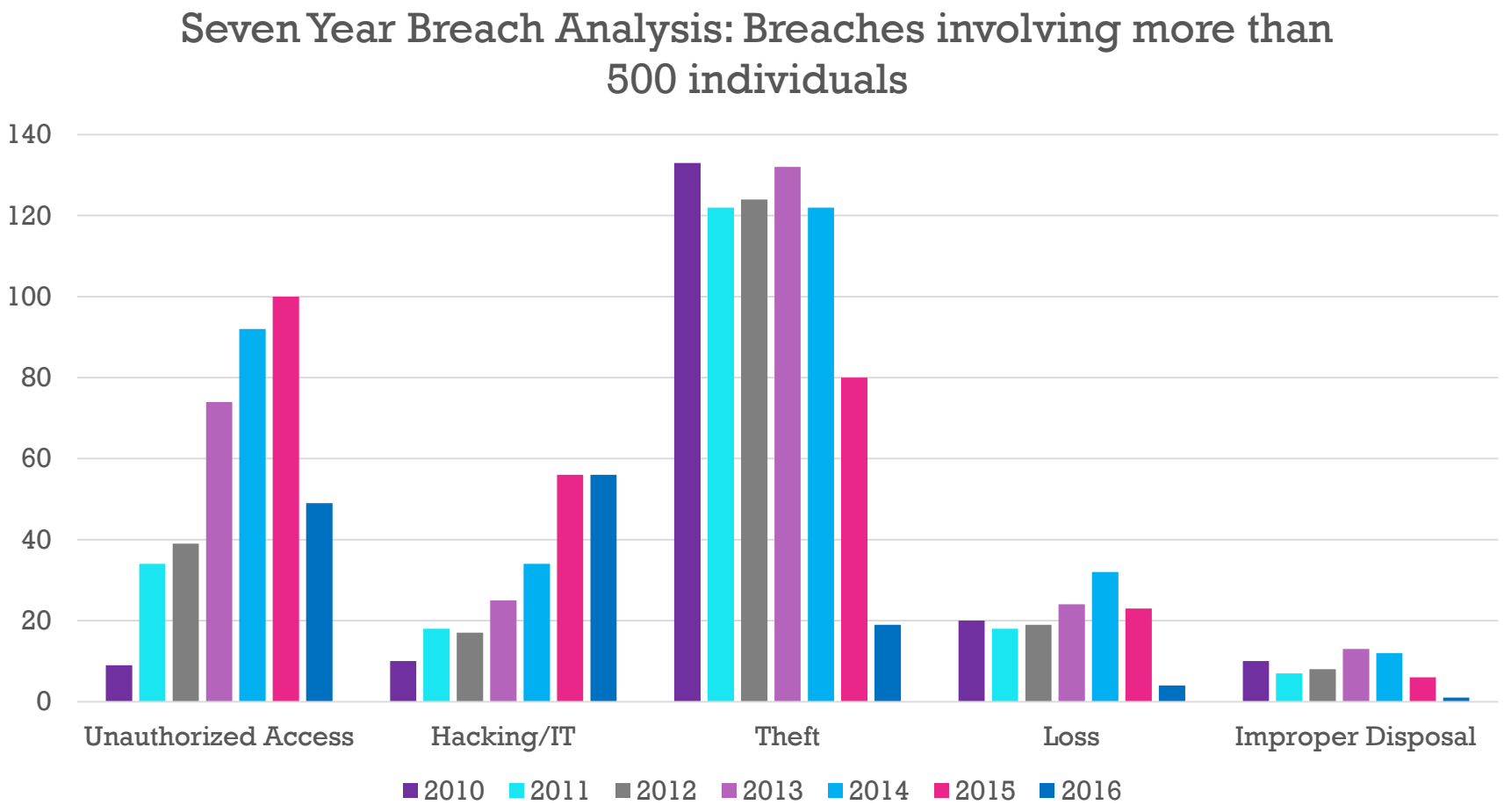
- Worth 10x more than credit card information
- Average of $363 per healthcare record

Why are We Vulnerable to Attacks?

Why Haven't We Addressed Security?

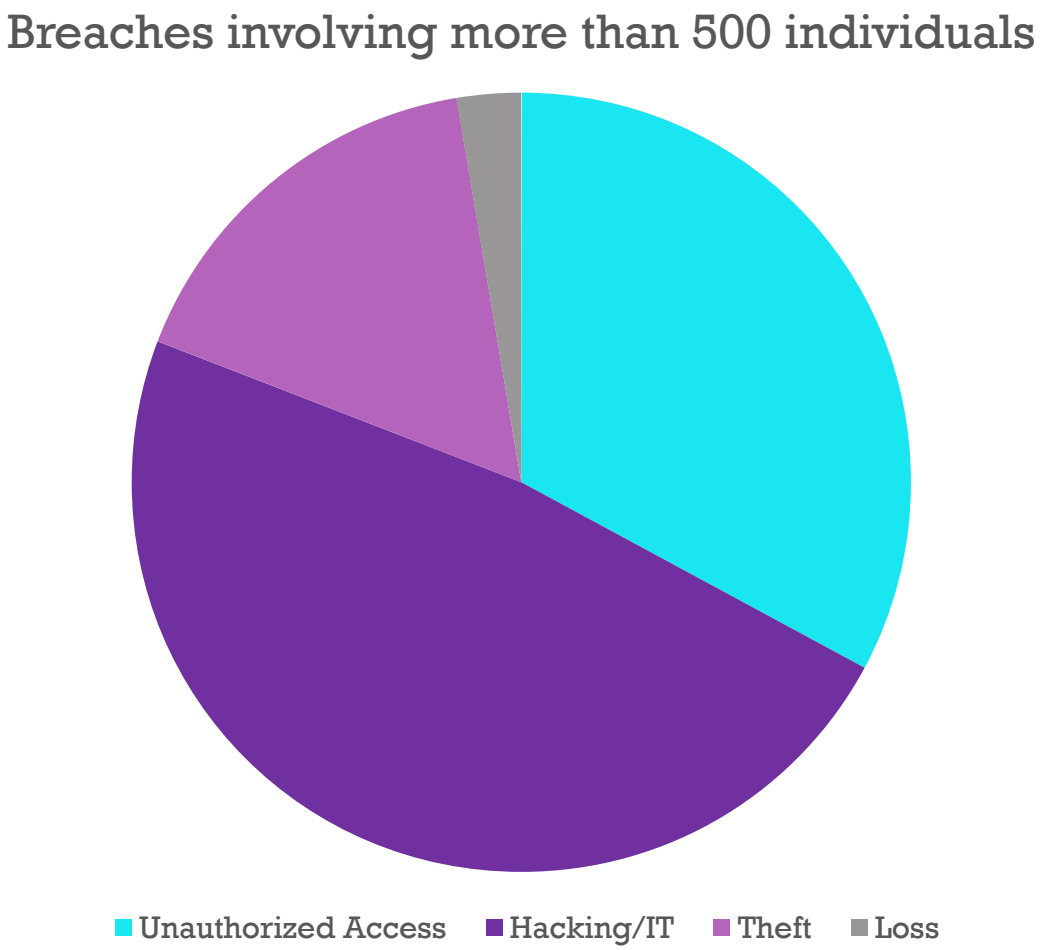
- Not viewed as critical to patient care
- Technology shortcuts are culturally "OK" in healthcare
- Budget – Tech is **expensive** to adopt and maintain
- Interruption of existing workflows are met with resistance

Understanding the Breaches in Healthcare



HIPAAtrek
Guiding Your HIPAA Compliance

2017 Breaches (so far…)



HIPAAtrek
Guiding Your HIPAA Compliance

Ransomware in Healthcare

- 72% of Hacking/IT incidents reported in 2016 were caused by Ransomware
- Ransomware has doubled in frequency across all industries
- Ransomware is the 5th most common malware attack
- Ransomware in healthcare is particularly concerning due to the need for rapid access to patient data
- Phishing and pretexting are the most common channel for ransomware attacks
  - Eagerness
  - Distraction
  - Curiosity
  - Uncertainty
- Ransomware-as-a-Service is now a thing

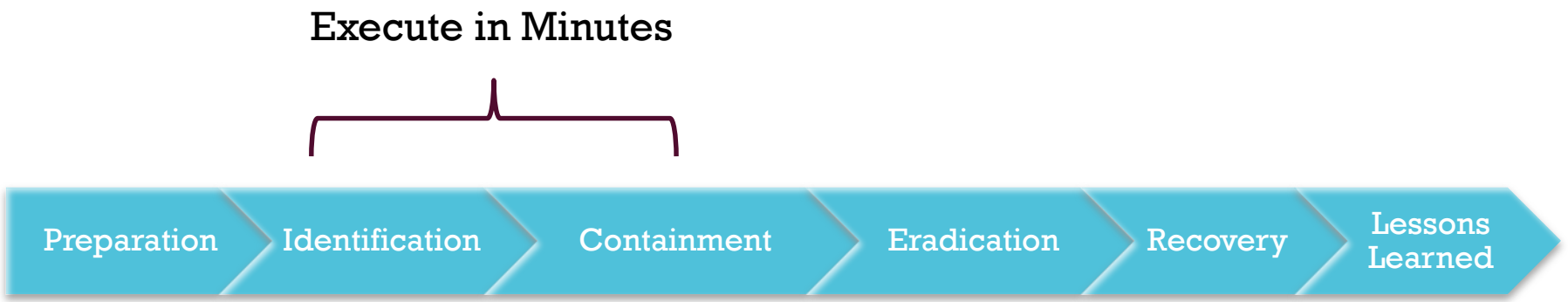
Mock Incident Response

- Your hospital is a victim of a ransomware attack
- Ransom being demanded to be paid within 40 hours in the form of Bitcoin – ransom will continue to increase after the deadline
- Team up!
- Walk through how you should respond – include security and compliance responses

Things to remember

- Define roles in your group. Consider this your Incident Response Team. Who is responsible for what?
- You can determine the type of ransomware attack you are responding to, the location of the attack, and the cause of the attack.
- The attack must have affected 500 individuals or more
- Include an after action report or lessons learned report (bullet points of items to be included in the report)
- Do you pay the ransom?
- Have you determined if it is a breach under HIPAA?

SANS Institute PICERL Approach for Ransomware Response



PICERL: Preparation

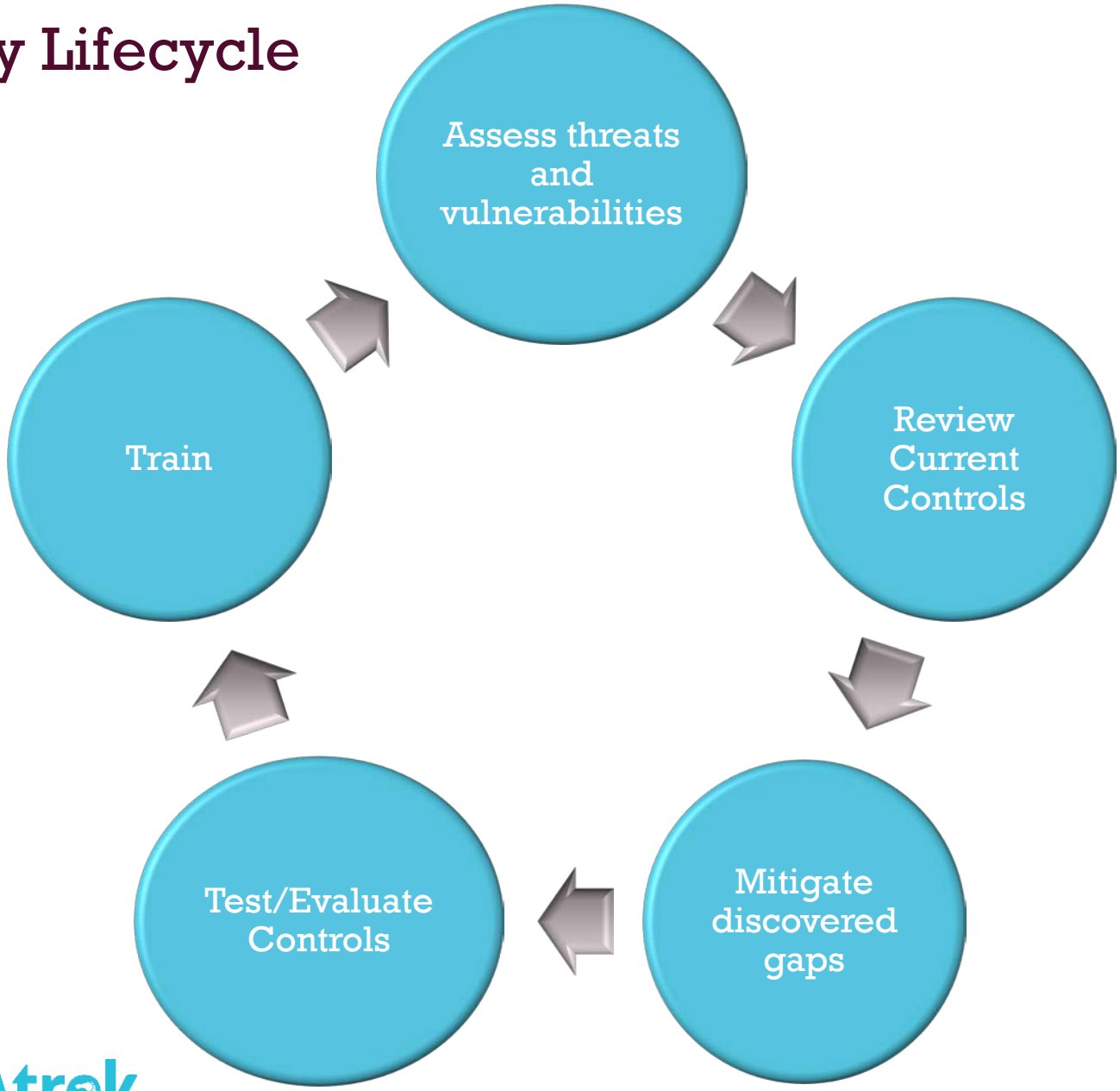
Sets the stage PRIOR to an incident

- Policies and Procedures
  - Think BEYOND HIPAA!
  - Security-Focused, compliance will follow
- Multi-disciplinary Incident Response Team
  - IT and Non-IT stakeholders
  - Key decision makers and non-decision management
- Routine risk assessments and audits
- Strengthen web and email gateways

PICERL: Preparation (cont)

- Training and Testing
  - More than just employee computer-based modular training
  - Social Engineering penetration testing – send a mock phishing attempt
- Solid Backup Plan
  - Use drives not mounted to a single computer or networked server
  - Segregate users from backups
  - Tiered approach to back-ups
  - A crisis is a bad time to explain why a backup is a week old and you've lost a week's worth of treatment records and other data
- Train and drill on downtown operating procedures

Policy Lifecycle



HIPAAtrek
Guiding Your HIPAA Compliance

PICERL Preparation Best Practices

An ounce of prevention…

- Ensure you have the correct Incident Response Team!
- IRT should be active in the Policy Lifecycle and creation/modification of security policies
- Consider an Incident Response Plan kit
  - Detailed plan
  - Checklists
  - Stakeholder contact information
  - Emergency Plan
  - RPO and RTO defined and understood by IRT
- Don't wait for a security incident to test
- Application and Data Criticality Analysis imperative to the contingency planning process!

PICERL: Identification

This begins once the threat or attack is discovered.

- Anti-exploitware or Intrusion detection systems which scan and monitor systems, networks, and computers can be used to help identify threats that have exercised a vulnerability
  - Not all attacks can be detected or prevented IDS and anti-exploitware . Be sure to patch applications, including anti-exploitware,
- Users may notify you of suspicious activity or if they are unable to access a workstation after a ransomware attack
- Audit of security logs can reveal malware that slipped through the cracks of your security program.
- Audits of workstations and networked systems can also uncover cybersecurity incidents.

Steps in the identification process are continuous procedures that make up a strong security protocol.

PICERL: Identification

Create a checklist for incident first responders

- Date
- Time
- Description – include type of attack, if possible
- First sign of incident
- Patterns, if any
- How many affected individuals (PHI, PII)?
- What is the extent of the incident?
- Where did the alert originate from?
- Who reported it?
- Who first responded?

PICERL: Containment

In ransomware attacks, by the time IT arrives it is too late!

- Train users to identify ransomware attacks and train them how to contain the infection
- Clear action plan to contain networked machines
- Use applications and data criticality analysis to assist in the containment process
- Containment can be concurrent with Identification

PICERL: Eradication

- This is the cleanup process that begins only after containment has occurred
- For ransomware attacks, going ”bare metal” is suggested by many security experts
  - Do not expect anti-exploitware to determine if the threat is completely eradicated
- Determine if third party involvement is needed
- Run a series of validation tests to ensure the problem has ceased
  - Ensure no gaps or backdoors have been forgotten

PICERL: Recovery

- Enact your disaster recovery plan!
- Recovery Point and Time Objectives
- Test to ensure proper recovery
- Determine and document what, if any, data has been lost

PICERL: Lessons Learned

- Compile documentation from security incident response
- Review documentation
- Make recommendations on how to prevent future similar attacks
- Create a risk management action plan around the incident
- Enact Breach Notification Policy
  - Report, if required, to state and federal officials, including the OCR
  - Notify any affected individuals

Ransomware Decision: To Pay or Not to Pay?

FBI discourages paying ransom:

- It is a criminal business model
- It does not guarantee you will receive the keys
- The ransom demand could increase
- It does not exempt your hospital from a second demand
- It does not prevent a secondary malware attack
- You may be able to negotiate a smaller ransom

Ransomware Decision: Is it a Breach?

- HHS released its guidance on Ransomware in 2016
- Ransomware attacks are deemed a security incident under the Security Rule
- Incident Response Team should treat Ransomware attacks as a potential breach of PHI
- It may be impossible to determine if ransomware attacker accessed PHI, seek legal council
- Conduct risk assessment around the attack
- Report to OCR within 60 days

Resources

Incident Response Cheat Sheets (SANS Institute):
https://isc.sans.edu/forums/diary/2+Cheat+Sheets+for+Incident+Handling/5354

OCR Ransomware Fact Sheet:
https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

OCR Cybersecurity Guidance:
https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

Sarah Badahman
sarah@hipaatrek.com
314-272-2600

HIPAAtrek
Guiding Your HIPAA Compliance