HEALTH CENTER CYBERSECURITY DEFENSE AND RESPONSE

Steps to Assess and Improve Cybersecurity Preparedness

Presented in partnership with the Washington Association for Community Health ~ June 15th, 2021

Washington Association for Community Health
Community Health Centers Advancing Quality Care for All

HEALTH INFORMATION TECHNOLOGY, HITEQ EVALUATION, AND QUALITY CENTER

Intro to HITEQ

The HITEQ Center is a HRSA-funded National Training and Technical Assistance Partner (NTTAPs) that collaborates with HRSA partners including Health Center Controlled Networks, Primary Care Associations and other NTTAPs to engage health centers in the optimization of health IT to address key health center needs through:

- A **national website** with health center-focused resources, toolkits, training, and a calendar or related events.
- **Learning collaboratives, remote trainings,** and **on-demand technical assistance** on key content areas.

email us at hiteqinfo@jsi.com!

HITEQ Topic Areas

Access to comprehensive care using health IT and telehealth

Privacy and security

Advancing interoperability

Electronic patient engagement

Readiness for value based care

Using health IT and telehealth to improve Clinical quality and Health equity

Using health IT or telehealth to address emerging issues: behavioral health, HIV prevention, and emergency preparedness

Introducing Nathan Botts

- Senior Study Director – Healthcare Delivery Research and Evaluation, Westat
- Health informatics and cybersecurity specialist
- Over 11 years of clinical software and systems research and development experience
- Privacy & Security lead for the HRSA HITEQ Center
- Professor of Cybersecurity ~ Purdue University Global

Nathan Botts, PhD, MSIS

HEALTH INFORMATION TECHNOLOGY, HITEQ EVALUATION, AND QUALITY CENTER

Legal Disclaimer

- The information included in this presentation is for informational purposes only and is not a substitute for legal advice.

- Please consult an appropriate attorney if you have any particular questions regarding a legal issue.

Health Center Cybersecurity Problem Statement

- Increased use of electronic health record systems increases security risk
- Increased use of IoT enabled mobile health and medical devices increases security risk
- Increased use of internet-based systems increases security risk
- Increased numbers of users on a given system increases security risk
- *That can be a lot of security risks for small to medium-sized health centers to effectively manage!*

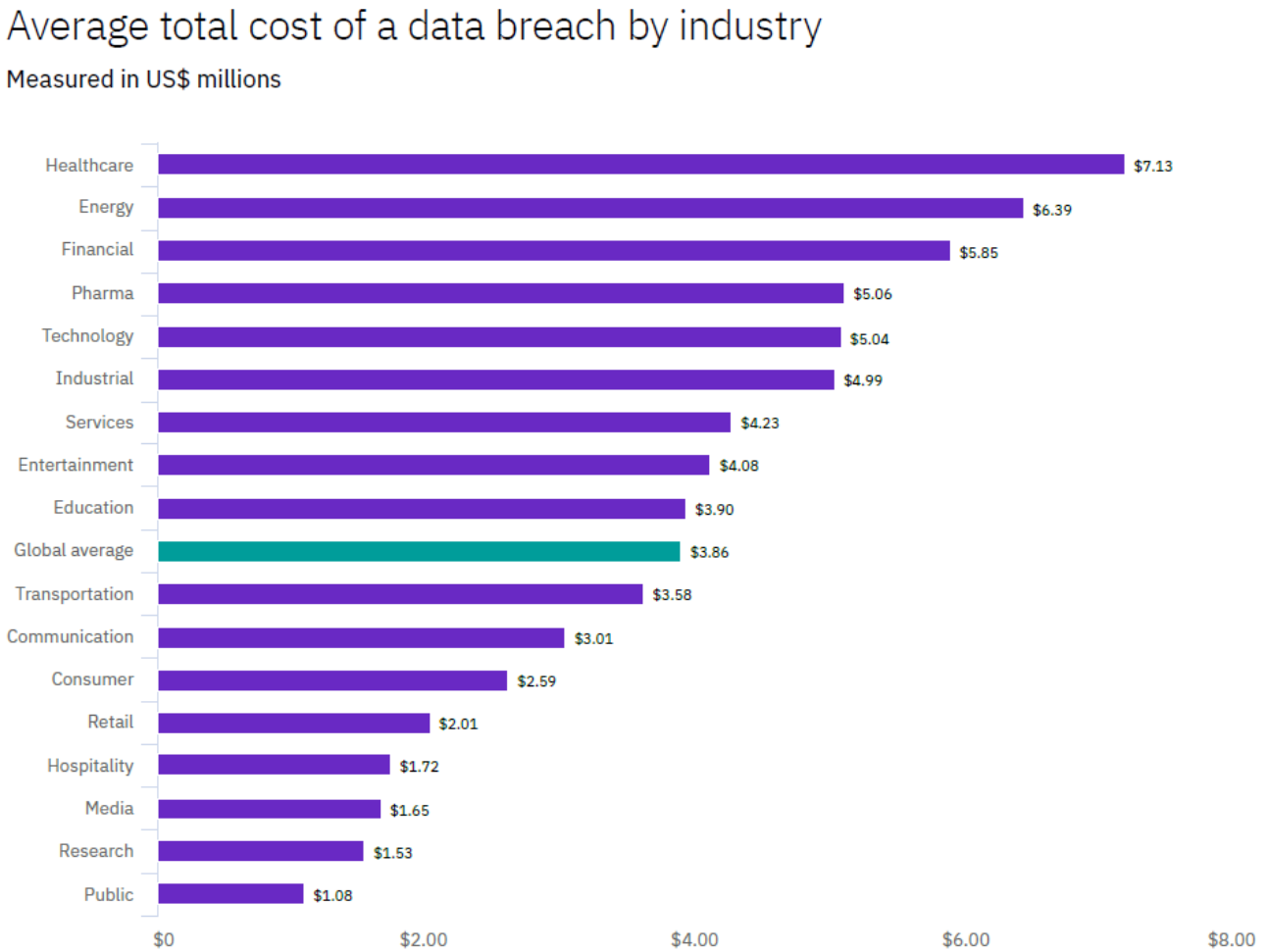
The Continued Rise of Ransomware

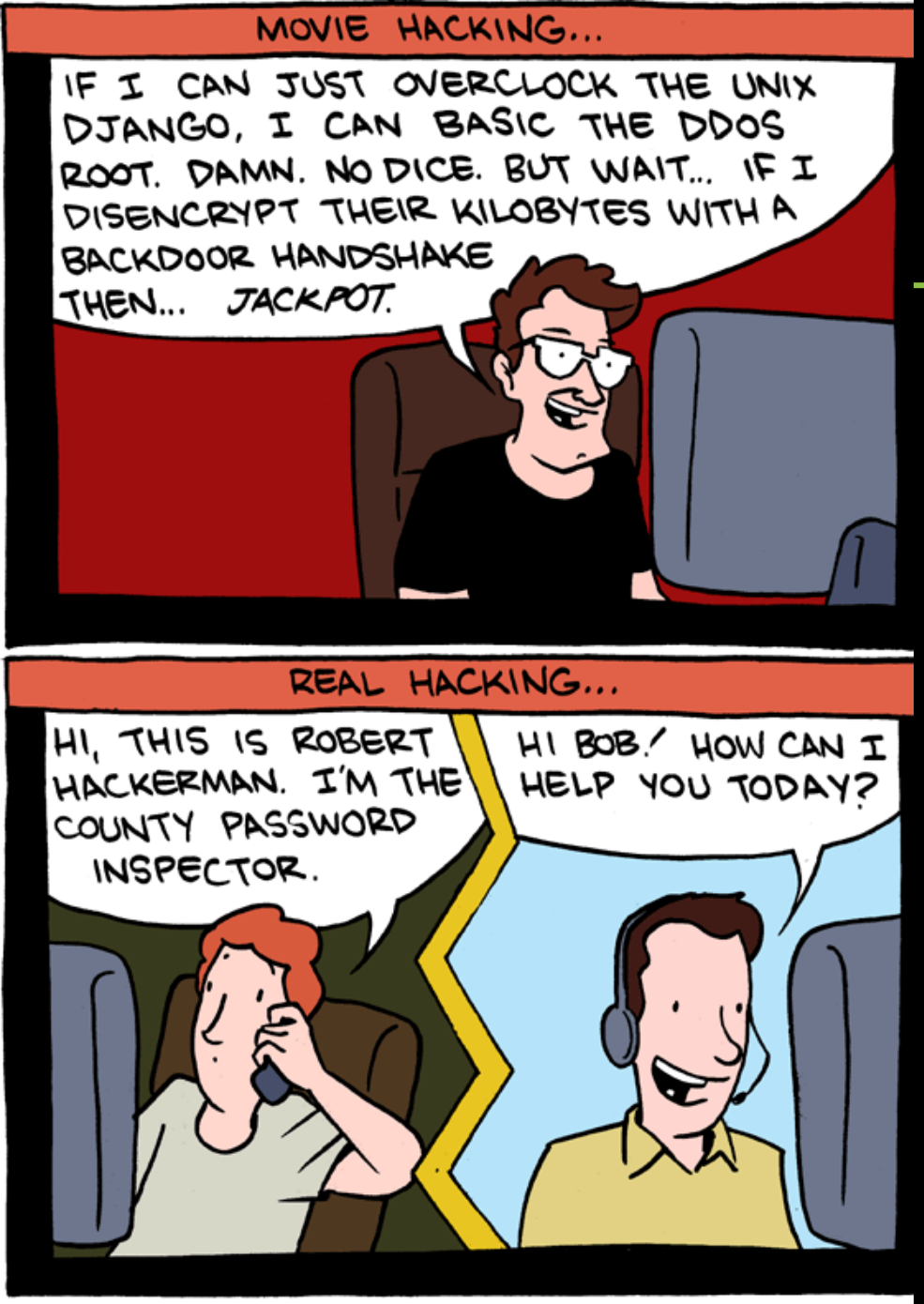
- The frequency of daily ransomware attacks increased 50 percent during the third quarter of 2020 from the first half of the year
- The effects can be seen in the most recent ransomware attack on Universal Health Services, which impacted all 400 US sites
- Educating the healthcare workforce on how to identify and avoid potential ransomware attacks is considered the most important defense against these attacks as the threat becomes more targeted via social engineering

US Ransomware Attacks Doubled in Q3; Healthcare Sector Most Targeted

New Check Point research examines the ransomware threat landscape for Q3 2020, noting a 50 percent increase in daily attacks. The healthcare sector is the most targeted globally.

The Cost of Healthcare Breach





Entry Points

- Phishing
- Ransomware
- Connected Medical Devices (IoT)
- Social Engineering
- Misconfigured Servers
- Inadvertent Disclosures
- Unpatched Systems
- Vendors and Business Associates
- Facilities and other supporting systems

Security Governance Models

1. Assume Breach
2. Defense in Depth
3. Risk-based Approach
4. Detection and Response
5. Continuous Improvement

Critical Security Controls and HIPAA

Control Family	HIPAA Security Rule Controls
CSC #1: Inventory of Authorized and Unauthorized Devices	164.310(c): Workstation Security - R 164.310(d)(1): Device and Media Controls: Accountability - A
CSC #2: Inventory of Authorized and Unauthorized Software	164.310(c): Workstation Security - R
CSC #3: Secure Configurations for Hardware and Software	164.310(c): Workstation Security - R
CSC #4: Continuous Vulnerability Assessment and Remediation	164.308(a)(8): Evaluation 164.308(a)(6): Security Incident Procedures
CSC #5: Controlled Use of Administrative Privileges	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R 164.312: Access Control: Unique User Identification - R 164.312(b): Audit Controls 164.312(d): Person or Entity Authentication

Security Rule Requirements

Security Components	Example Variables	Example Security Measures
Physical Safeguards	• Facility structure • Data storage center • Computer hardware	• Building alarm system • Locked doors • Monitors shielded from view
Administrative Safeguards	• Designated security officer • Staff training and oversight • Information security control • Security Risk Assessment / review	• Staff training • Monthly review of user activity • Policy enforcement • New hire background checks
Technical Safeguards	• Controls on access to EHR • Audit log monitoring • Secure electronic exchanges	• Secure passwords • Data backup • Virus scans • Encryption
Policies and Procedures	• Written P&P addressing HIPAA Security requirements • Documentation of security measures	• Written protocols on safeguards • Record retention • Periodic policy and procedure review
Organizational Requirements	• Breach notification and other policies • Business Associate agreements	• Periodic Business Associate Agreement review and updates

Security Risk Assessment

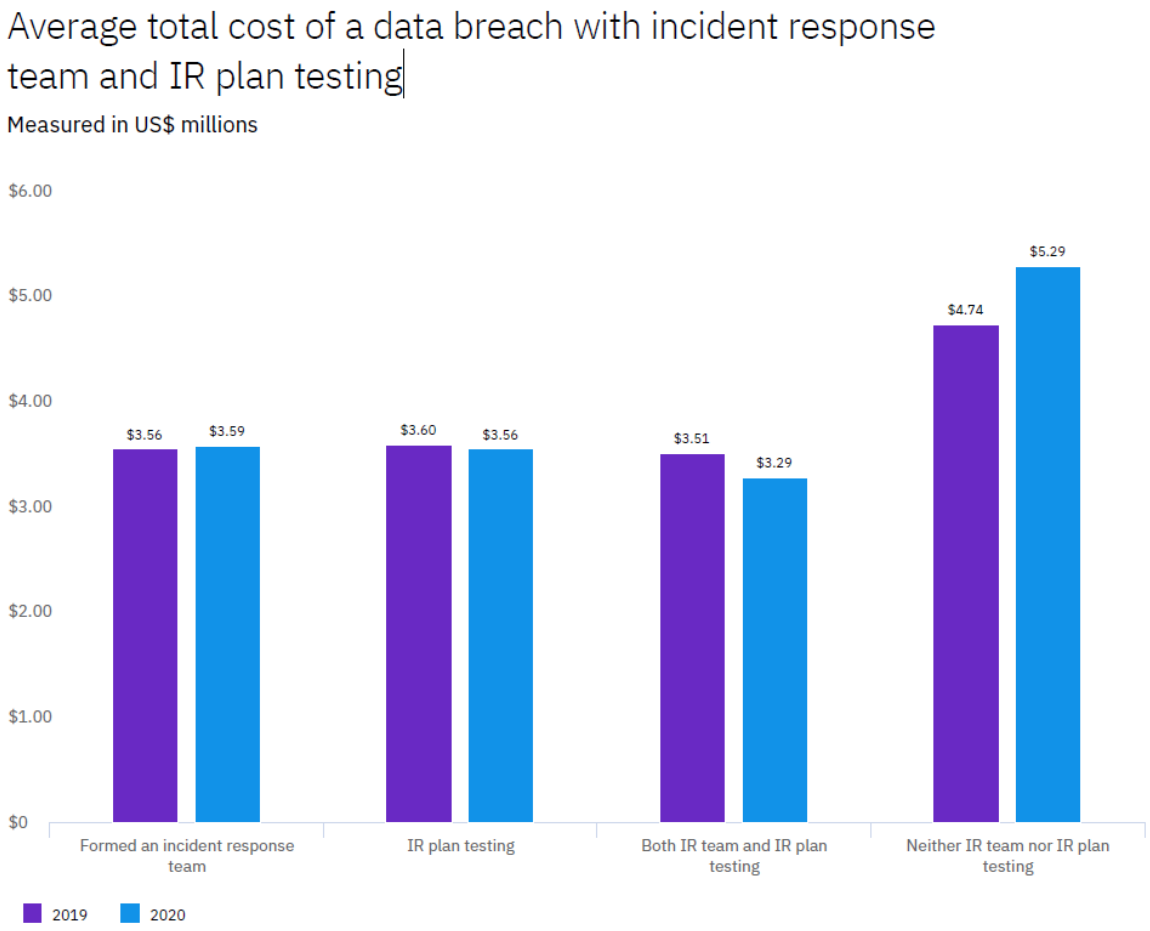
- Teach everyone in your health center to love the SRA
- Make everyone in your health center be a part of conducting a SRA
- By conducting an SRA regularly, providers can identify and document potential threats and vulnerabilities related to data security, and develop a plan of action to mitigate them.
- You cannot protect what you are unaware of!

Cyber Insurance Considerations

- Some policies do not cover the costs to prepare notifications to OCR or the penalties imposed.
- Others may not cover lost revenue due to suspension of services during a ransomware attack.
- Cyber-insurance market is evolving constantly as the nature of cyber-threats change.
- What scenarios are not covered and how can your organization mitigate for those risks?
- How robust is your incident response plan? A robust IRP can greatly assist in mitigating the financial impact to an organization.

Security Incident Response Planning

The Cost of Not Being Prepared



Incident Response Readiness Table Top Exercise Activity

Exercise Overview

- For those of you unfamiliar with the term, a Table Top Exercise is a small but inclusive exercise that occurs as part of Information Security's attempt to be better prepared to respond to potential cyber related incidents.

- The Table Top Exercise serves to exercise preparedness, validate plans, test operational capabilities, maintain leadership effectiveness, and examine the ways the organization works with the larger community outside of the company to prevent, protect from, respond to, recover from, and mitigate cyber related incidents.

Incident Response Scenario – Ransomware Attack

- A phishing email was sent to numerous members of the medical practice
- One person clicked on the link and entered their credentials into the attacker's fake website
- Shortly after, the victim's computer displayed a ransom message
- The user reported the incident to the IT helpdesk

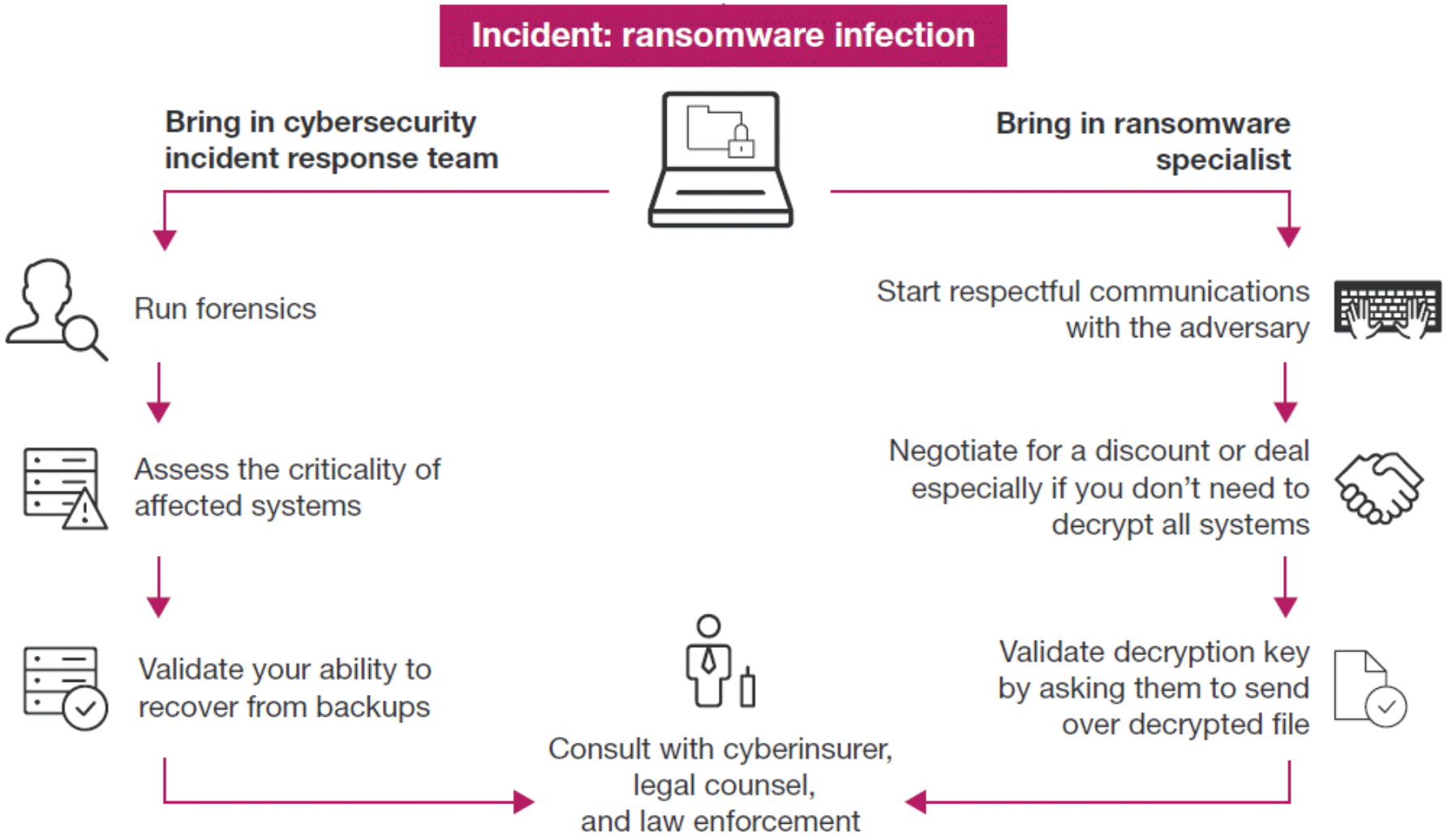
The Fallout

- Beyond the computer systems that have been encrypted, you are experiencing clinical support computers that are receiving data slowly, do not respond, or freeze.
- Patient care is increasingly delayed as physicians and clinicians authenticate and verify patient EHR/EMR information through labor intensive and time-consuming, downtime manual paper procedures. (e.g., patient questioning, contacting families).
- Amidst the treatment of patients with corrupt EHRs/EMRs, the center becomes rapidly overwhelmed and as new patients arrive, only life-threatening emergencies are accepted for emergency department treatment.
- Trauma staff members are complaining that the EHR/EMR system has virtually ground to a halt and is unusable. Administrator priorities shift to reaffirming EHR/EMR data integrity.

Potential Questions to Ask

- If you are the one who receives the ransomware notification what is the first thing you should do?
- How are you going to document the steps that are taken?
- Do you have a crisis management team that should be activated? If yes, who would initiate the activation?
- When should Senior Leadership be notified?
- When do you contact law enforcement? Who?
- What would your strategy be if it looks like you will only lose one day's worth of data?
- Assume a recent backup is not recoverable. The 6-week backup appears to not be impacted but it may take 1½ weeks to recover the data. Is using a 6-week backup a viable option to pursue?
- What would be the strategy to continue business for 1½ weeks?
- What actions should non-IT areas consider? How will these actions be coordinated with other key partners?

Debrief: Ransomware Response Report



Get Your Badge!

1. Thanks for your participation!
2. Visit: http://bit.ly/hiteq-defender
3. Fill out the Health Center Defender Against the Dark Web Badge Confirmation form
4. Receive your badge!

Questions? Feedback?

Email: hiteqinfo@jsi.com

Phone: 1-844-305-7440

This project is supported by the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS) as part of an award totaling $778,000 with 0 percentage financed with non-governmental sources. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by HRSA, HHS, or the U.S. Government. For more information, please visit HRSA.gov.