Healthcare Cybersecurity Policy Update

September 2016

pwc

Ransomware – A Definition

- Ransomware is a type of malware (malicious software) that denies access to data by encrypting the data with a key known only to the attacker who deployed the ransomware.
- After a user's data is encrypted, the ransomware directs the user to pay a ransom (usually in a cryptocurrency, such as Bitcoin) in order to receive the key to decrypt the user's data.
- Even if ransom is paid, the ransomware attacker may not provide the key to decrypt the data or may increase ransom demands.

Audience Poll - Is a Ransomware Attack a *Breach?*

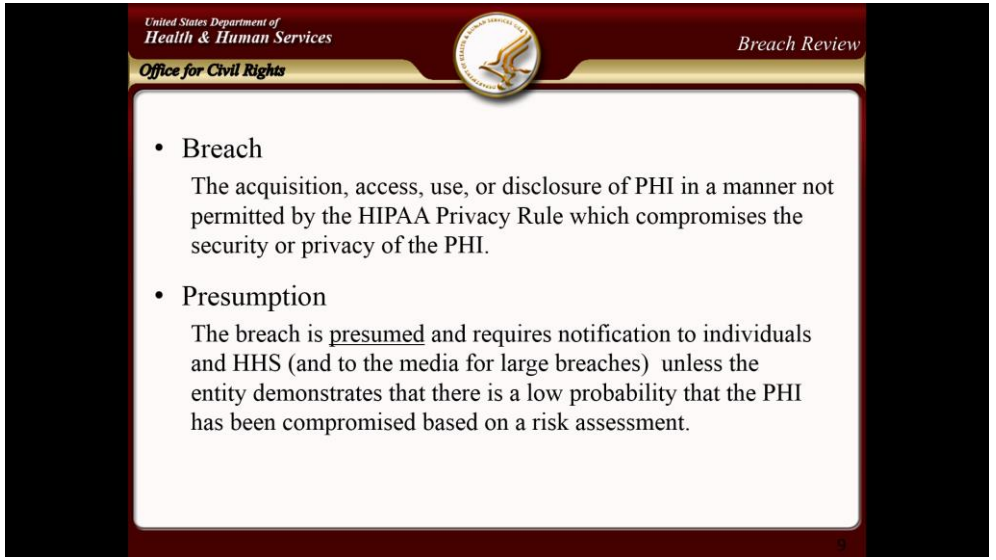
1. Yes
1. No
2. Not clear until analysis is accomplished

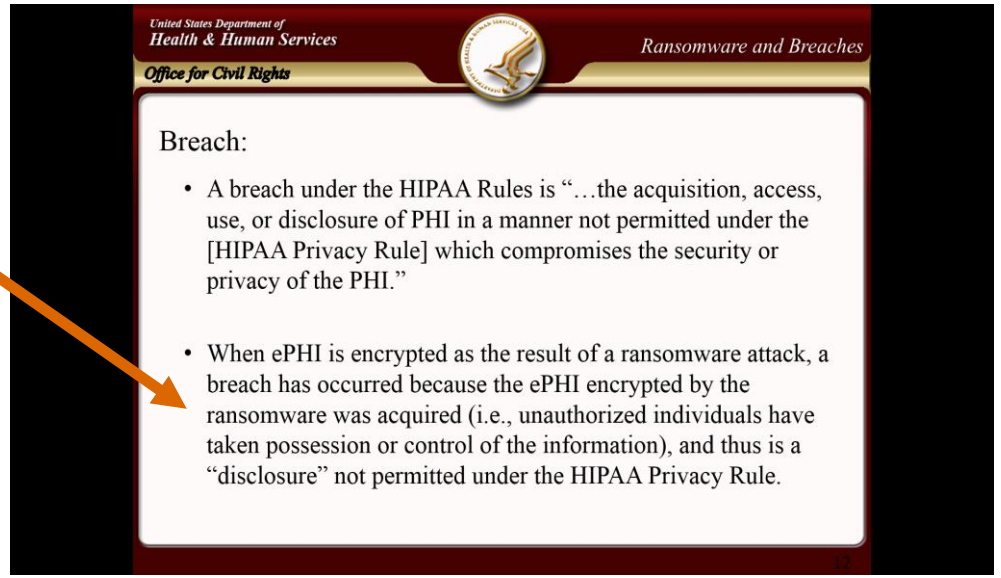
Is a Ransomware Attack a *Breach?*

The answer is: YES

A Ransomware Attack is a *Breach because…*

When the data is *encrypted*, the data was “acquired” (control of the information is taken) and thus is “disclosed” to the perpetrator.





Discussion Points

- **Federal Law**
  - CISA of 2015
  - Passed Bills/Hearings
- **Regulation/Regulatory Activity**
  - HHS OCR - Ransomware
  - DHS/HHS ASPR – ISAOs standards/guidance
  - Other
- **State Law**
  - Data Breach Notification Laws
  - Cyber Laws

Cybersecurity Information Sharing Act of 2015

Passed as part of the part of the FY2016 omnibus spending package

- **Secs. 105-106** - creates new legal authorizations and protections for the sharing of cyber threat indicators and defensive measures between and within the private sector and the government.
  - Monitor and Defend Information Systems
  - Share or Receive Cyber Threat Indicators or Defensive Measures
  - Requires a Scrub Personal Information Before Sharing
  - Provides Protections for Sharing and Receiving Information (As Applicable)
  - Protection from Liability, Antitrust Exemption, Non-Waiver of Privilege, Proprietary Information, Exemption from Federal and State FOIA Laws, Information Cannot Be Used to Regulate or Take Enforcement Actions Against Lawful Activities,

  Provides Federal Guidance for Sharing Cyber Threat Indicators and Defensive Measures for the Private Sector

CISA of 2015 (cont.)

- **Sec. 204 -Information Sharing and Analysis Organizations**. (more on next slide)
  - Recognizes the role of ISAOs and adds certain cyber risk definitions to section 212 of the Homeland Security Act of 2002 (6 U.S.C. 131).
- **Sec.405** - Provisions for HHS action include the development of:
  - A plan within each division of the Department of Health and Human Services spelling out responsibilities for addressing cyberthreats in the healthcare sector;
  - An HHS industry task force to examine, among other things, the cyber challenges facing the healthcare sector, as well as lessons the sector can learn from other industries;
  - A common set of voluntary consensus-based guidelines, best practices and methodologies to help healthcare organizations better address cyberthreats.

DHS - ISAOs

- **Executive Order 13691**, Promoting Private Sector Cybersecurity Information Sharing, directs DHS to:
  - Develop a more efficient means for granting clearances to private sector individuals who are members of an ISAO via a designated critical infrastructure protection program;
  - Engage in continuous, collaborative, and inclusive coordination with ISAOs via the DHS National Cybersecurity and Communications Integration Center (NCCIC), which coordinates cybersecurity information sharing and analysis amongst the Federal Government and private sector partners; and
  - Set-up an ISAO Standards Organization to identify a set of voluntary standards or guidelines for the creation and functioning of ISAOs.
- **DHS Automated Indicator Sharing (AIS) program***
- **ISAO standards organization – draft standards soon**

* - https://www.us-cert.gov/ais

Recent Bills/ Hearings/Proposed Legislation

- **Senate HELP Committee Passes "Improving Health IT Act"**
  - Establishes a star-rating system for EHRs based on security, usability and interoperability
- **Senate HELP Committee Passes "MEDTECH Act"**
  - Aims to boost innovation in health IT by exempting low-risk medical software and mobile apps from regulatory oversight. Security still a challenge.
- **House Oversight Committee Hearing Explores Health IT Interoperability, Meaningful Use, and Ransomware**
  - Concerns that the HITECH security breach notification requirements do not appear to explicitly address situations in which patient data is frozen in storage by attacker
  - Need for separate legal/regulatory action on Ransomware?

Recent Bills/ Hearings/Proposed Legislation (cont.)

- **Industry Panel on Ransomware**
  - Senate Health, Education, Labor and Pensions – in oversight role
- **E&C Subcommittee on Oversight and Investigations Hearing**
  - entitled “Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives.”

Other

- **Obama Administration's Cybersecurity National Action Plan**
  - Cybersecurity National Action Plan collaborating with health insurers and healthcare stakeholders to better secure their information systems.
  - Commission on Enhancing National Cybersecurity
- **HHS**
  - ONC FACA Committees – HITPS/HITSC Joint Hearings on API Security, PMI Data security
  - Office of Secretary - Cybersecurity Task Force
  - FDA - Guidance to medical device vendors on threat information sharing
- **NIST seeking grant applications**, as part of the National Strategy for Trusted Identities in Cyberspace (NSTIC) *Federated Identity in Healthcare Pilot Program*, to:
  - demonstrate the usage of federated online identity solutions for patients and providers across multiple healthcare providers (e.g., provider groups, regional healthcare systems, hospital systems).
  - Grantees must provide data on how they implemented the solution and how it performed, ultimately contributing to a jointly published document that can serve as a guide for other healthcare systems.

Other (cont.)

- **"Interagency Cybersecurity Forum for Independent and Executive Branch Agencies"**
  - FCC, FTC, NRC
  - Mission: De-conflicting" agencies' approaches to cybersecurity and "streamlining" rules (regs.)
  - Will provide recommendations soon.
- **FTC Interactive Website provides "Mobile Health Apps Interactive Tool*"**
  - Helps you determine what federal laws apply to a particular mobile health app
  - HIPAA, FD&C Act, FTC Act, FTC Health Breach Notification rule
- **DHS' Cyber Storm V - annual cybersecurity exercise with simulated cyber event**
  - Healthcare sector and HHS participate for first time

* - https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool

States move on Cyber Laws

- **Breach Notification**
  - **Forty-seven states**, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private, governmental or educational entities to notify individuals of security breaches of information involving personally identifiable information.

    http://www.ncsl.org/research/telecommunications-and-information-technology/overview-security-breaches.aspx
- **Cybersecurity**
  - States are addressing cybersecurity through various approaches, such as:
    - Creating cybersecurity commissions, studies or task forces,
    - Requiring government or public agencies to implement security practices,
    - Offering incentives to the cybersecurity industry, and/or
    - Promoting cybersecurity education.

    http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2016.aspx

Questions?

Lisa Gallagher
Managing Director
PwC Health Industries Privacy and Cybersecurity
Lisa.A.Gallagher@pwc.com