



Ransomware Attacks on U.S. Healthcare

Law Enforcement, Regulatory, Legal
& Cybersecurity Perspectives



**LITIGATION
CONFERENCES**

Ben Goodman, 4A Security & Compliance
Sean Hoar, Lewis Brisbois Bisgaard & Smith LLP
Barbara Holland, OCR, U.S. Department of Health & Human Services
Benjamin Stone, Cyber Desk, Federal Bureau of Investigation

General Webinar Announcements

- Welcome!
- Asking questions
 - Please submit via text box
- Getting CLE
 - CLE@LitigationConferences.com
- Getting the PowerPoint and recording
- Contact HB
 - Tom.Hagy@LitigationConferences.com
- This is for educational purposes only

**RANSOMWARE ATTACKS
AGAINST U.S. HEALTH CARE**

**LAW ENFORCEMENT,
REGULATORY,
LEGAL &
CYBER SECURITY PERSPECTIVES**

CHAIR & MODERATOR

BEN GOODMAN

President, 4A Security & Compliance

SPEAKERS

SEAN HOAR

Partner, Lewis Brisbois,
Chair of the Data Privacy & Cybersecurity Practice

BARBARA HOLLAND

Barbara Holland, Regional Manager, HHS OCR

BENJAMIN STONE

Supervisory Special Agent, Cyber Desk, FBI

TODAY'S FACULTY

CHAIR & MODERATOR



Ben Goodman, President, 4A Security & Compliance

- Leads the 4A team of information security, incident response, IT audit, risk management and compliance professionals
- 25+ years in IT, technology strategy, security and risk management
- Specialization in healthcare security & compliance
- Comprehensive breach response services
- Faculty Member at Drexel University, LeBow School of Business
- Host of [4A Healthcare Data Security & Privacy Symposium](#), March 22nd, 2018



SPEAKERS

Sean Hoar, Partner, Lewis Brisbois

Chair of the Data Privacy & Cybersecurity Practice



- CISSP, GISP, CIPP/US;
- Extensive experience managing responses to digital crises and effectively marshalling resources to contain and remediate information security incidents;
- Served as the lead cyber attorney for the U.S. Attorney's Office in Oregon where he was the point of contact for the FBI, Secret Service, and Homeland Security in system intrusions and other digital crime emergencies;
- Counsels businesses on best practices in information privacy and data security, and countering cybersecurity threats;
- Facilitates incident response planning and risk assessments, and manages responses to data breaches;
- Veteran security and privacy attorney and an accomplished litigator prosecuting cybercrime, identity theft, Internet fraud, and other matters for the U.S. Department of Justice, managing compliance with the Fourth Amendment, the Stored Communications Act, and other constitutional and regulatory frameworks for federal law enforcement;
- Trained federal investigators and prosecutors about the acquisition and use of digital evidence, and he trained foreign officials, on behalf of the U.S. Department of State, about anti-terrorism and cybercrime awareness;
- Currently teaches courses in cybercrime and privacy law and serves as the executive director of the Financial Crimes & Digital Evidence Foundation;
- Author and speaker on privacy and security matters and received numerous accolades from the FBI, the Secret Service, the IRS, and the DEA throughout his career.

SPEAKERS



Barbara Holland, Regional Manager

U.S. Dept. of Health & Human Services, Office for Civil Rights

- Regional Manager for the Department of Health and Human Services Office of Civil Rights in October 2012
- Responsible for management and oversight of OCR's work enforcing both civil rights and HIPAA compliance in PA, DE, MD, WV, VA, and DC;
- Previously served as the Department's Deputy Executive Secretary, managing on behalf of the Secretary the review and thorough vetting of regulatory policies and decisions for the Affordable Care Act and other Department initiatives and the development and implementation of Department responses to Presidential Executive Orders and Memoranda on regulatory reform and regulatory agenda-setting;
- Before returning to HHS in 2010, Barbara worked almost eight years for Pennsylvania Governor Ed Rendell and, before that, had an active general law practice for over fifteen years;
- Barbara began her public service career at HHS and was one of the youngest members to be inducted into the United States Government Senior Executive Service. Barbara holds a bachelor's degree from Cornell University and a law degree from the University of Pennsylvania where she was an Editor of the Law Review. She also holds a Masters Degree in Public Health from Yale University.

SPEAKERS

Ben Stone, Supervisory Special Agent FBI Cyber Squad



- Entered duty with the FBI in January 2002 and was assigned to the Houston Division, Texas City Resident Agency where he worked a variety of criminal matters;
- In April 2008, Mr. Stone was promoted to Supervisory Special Agent in the FBI's Weapons of Mass Destruction (WMD) Directorate where he supervised FBI programs related to the prevention of the proliferation of WMDs;
- In June 2010, Mr. Stone was named to the FBI's Philadelphia Field Office to serve as Supervisory Special Agent of the Intelligence Squad, responsible for the strategic recruitment of Confidential Human Sources across the Division;
- In February 2013, Mr. Stone was promoted to Assistant Inspector at FBIHQ where he served in the Office of Inspections and was responsible for conducting inspections across multiple FBI Field Offices and FBIHQ Divisions;
- In March 2014, Mr. Stone returned to Philadelphia and was chosen to lead the newly created Cyber Criminal Squad responsible for all criminal cyber crimes for the FBI Philadelphia Office;
- June, 2016, through January, 2017, Mr. Stone served at the US Embassy, Paris, France as the FBI's liaison to French Law Enforcement and Security Services regarding Cyber matters;
- Mr. Stone is a native of the United Kingdom and has a B.S. in Chemistry from the University of East Anglia and a M.S. in Organic Chemistry from the University of Pennsylvania. Prior to entering the FBI Mr. Stone worked as researcher in the pharmaceutical industry. Mr. Stone holds two United States Patents and is the author or co-author on several peer reviewed scientific papers.

LEARNING OBJECTIVES

RANSOMWARE ATTACKS AGAINST U.S. HEALTH CARE

FBI

- What are the latest ransomware trends the FBI seeing?
- What is the FBI's current ransomware damage assessment?

HHS OCR

- What is the HHS OCR stance on ransomware?
- What action does HHS OCR take upon receiving a ransomware incident report?

LEGAL

- What are the primary legal considerations during a ransomware incident?
- What are the most important steps a health care organization should take when a ransomware incident occurs?

CYBER SECURITY

- What makes some health care organizations less susceptible to damaging ransomware attacks
- What can they do to prevent and/or prepare for a ransomware attack?

INTRODUCTION

WHAT IS RANSOMWARE?

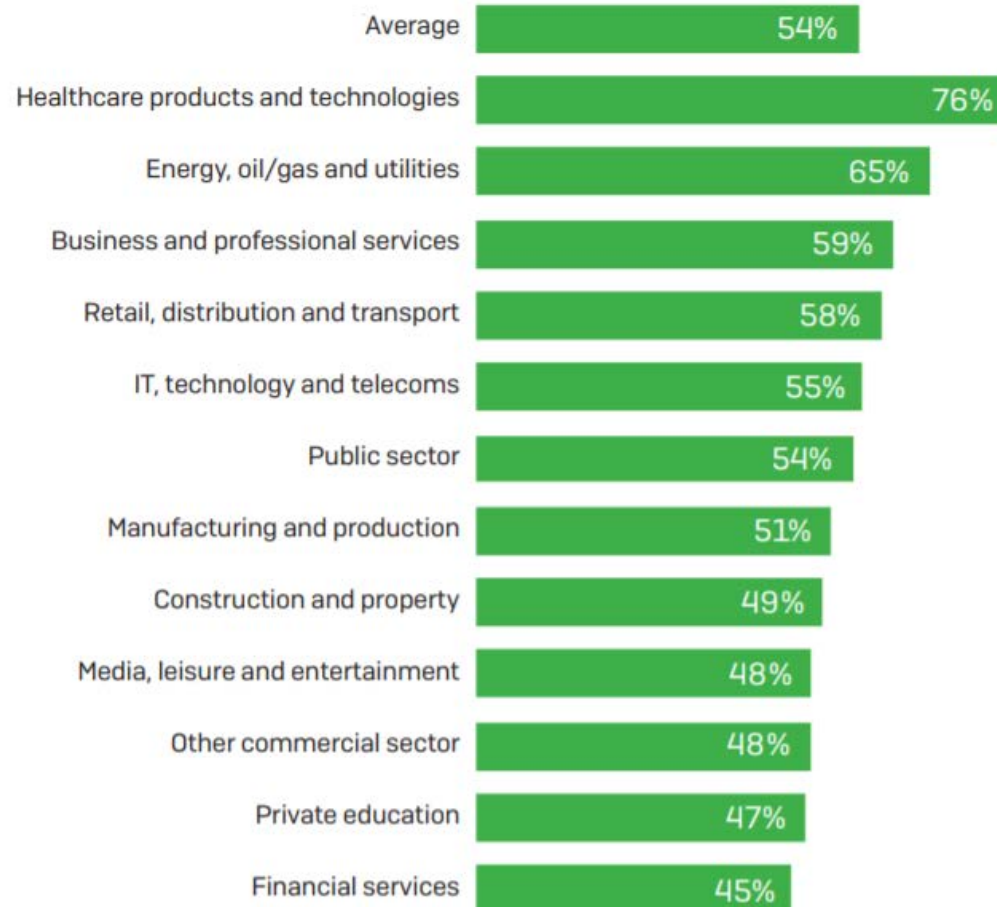
- A form of malicious software (malware) designed to:
 - Prevent access to your data, typically by encrypting it, but sometimes by completely removing it, especially if prompt payment isn't made
 - Provide ransom payment instructions and a means to receive a decryption key that can (theoretically) unlock and restore access to the data
 - Time element

WHAT IS RANSOMWARE?

- Hundreds of ransomware families and thousands of variants with many attack vectors
- New variants detected daily
- Often delivered via malicious attachments to fraudulent emails (Rapid Ransomware)
- Malvertisements (Ransom-GandCrab, Fake Flash Download)
- Direct attacks against servers (SamSam)
- “Contagious” spread from system to system (WannaCry)

WHAT IS RANSOMWARE?

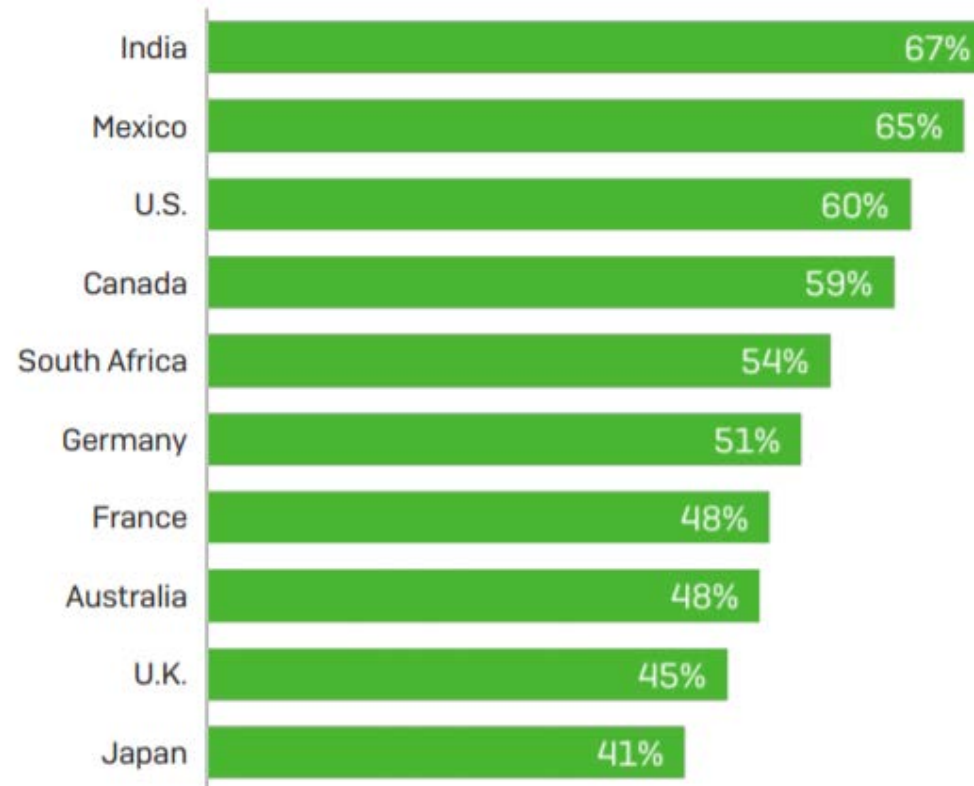
Hit by ransomware, by sector (n=2,700)



The State of Endpoint Security Today, Sophos, January 2108

WHAT IS RANSOMWARE?

Hit by ransomware, by country



The State of Endpoint Security Today, Sophos, January 2108

RANSOMWARE ATTACKS AGAINST U.S. HEALTHCARE

- 94% of medical institutions are victims of cyber attack*
- 75% of healthcare entities have been, or believe they have been the victims of ransomware attacks*

Major ransomware attacks against healthcare**

<u>2016</u>	<u>2017</u>
19	36

**Office of the Assistant Secretary for Preparedness and Response, U.S. Department of Health and Human Services between July 2015-June 2016*

*** Cryptonite*

RANSOMWARE ATTACKS AGAINST U.S. HEALTHCARE

January 2018: Hancock Health, Greenfield, Indiana

- Hit with SamSam ransomware
- Had back-ups but “recovery would take weeks”
- Paid 4 Bitcoin (~\$55,000)
- Recovered files – systems up and running 5 days after attack

RANSOMWARE ATTACKS AGAINST U.S. HEALTHCARE

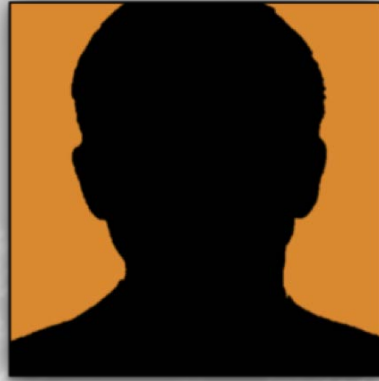
January 2018: Adams Health Network, Decatur, Indiana

- Hit with SamSam ransomware (same as Hancock Health)
- EHR and Scheduling encrypted
- Medical offices closed
- Did not pay ransom
- Restored systems in 4 days

RANSOMWARE ATTACKS AGAINST U.S. HEALTHCARE

January 2018: Allscripts, Raleigh & Charlotte, NC

- Two data centers hit with SamSam ransomware (unrelated variant)
- Hosted Pro EHR and hosted EPCS were encrypted
- Other systems “proactively shut down to protect client data”
- Didn’t pay ransom, restored from back-ups
- Outage lasted 4~6 days



LAW ENFORCEMENT PERSPECTIVE

SUPERVISORY SPECIAL AGENT BEN STONE,
FBI CYBER SQUAD

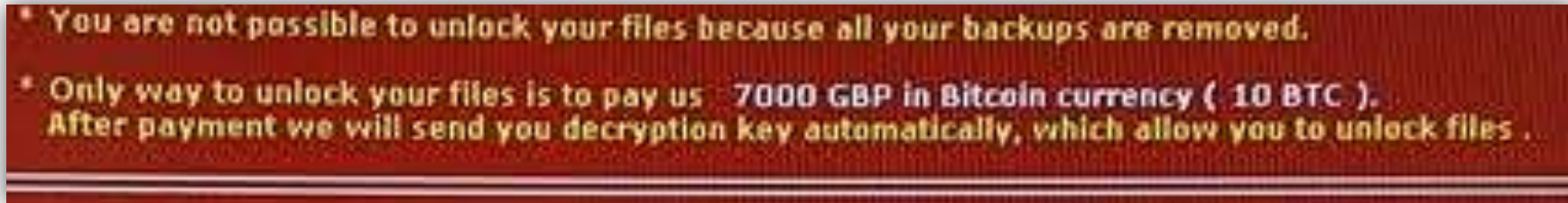
LAW ENFORCEMENT PERSPECTIVE - FBI

- What are the latest ransomware trends the FBI is seeing?
- What is the FBI's current ransomware damage assessment?

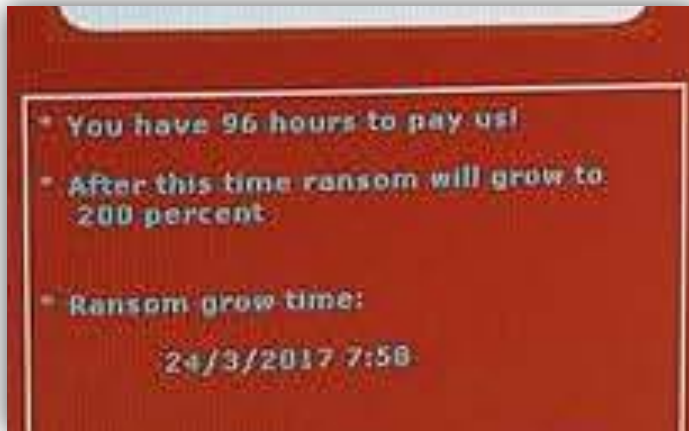


LAW ENFORCEMENT PERSPECTIVE - FBI

- What are the latest ransomware trends the FBI is seeing?
- What is the FBI's current ransomware damage assessment?



* You are not possible to unlock your files because all your backups are removed.
* Only way to unlock your files is to pay us 7000 GBP in Bitcoin currency (10 BTC).
After payment we will send you decryption key automatically, which allow you to unlock files .



* You have 96 hours to pay us!
* After this time ransom will grow to 200 percent.
* Ransom grow time:
24/3/2017 7:58

This variant: DMA Locker
Uses RDP to access systems

Other variants include:
Crysis, Darhma, Locky, SAMSAM

LAW ENFORCEMENT PERSPECTIVE - FBI

Some current trends

- Ransomware as a service (RaaS)
- Most Common Attack Vectors
 - Phishing
 - Drive-by downloads
 - Java



REGULATORY PERSPECTIVE:

BARBARA HOLLDAND, REGIONAL
MANAGER, HHS OFFICE FOR CIVIL RIGHTS

REGULATORY PERSPECTIVE

As of roughly February 25, 2018

Current

Under investigation greater than 500 all	400
Under investigation greater than 500 hacking/IT Incident	179
Under investigation greater than 500 hacking/IT Incident of network server	110

Archived

Archived greater than 500 all	1814
Archived greater than 500 hacking/IT incident	249
Archived greater than 500 hacking/IT of network server	170

REGULATORY PERSPECTIVE

Probability of Compromise

To demonstrate that there is a low probability that the protected health information (PHI) has been compromised because of a breach, a risk assessment considering at least the following four factors (see 45 C.F.R. 164.402(2)) must be conducted:

1. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. the unauthorized person who used the PHI or to whom the disclosure was made;
3. whether the PHI was actually acquired or viewed; and
4. the extent to which the risk to the PHI has been mitigated.

REGULATORY PERSPECTIVE

Helpful Info at:

- Helpful guidance at <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html>
- For guidance on making PHI unusable, etc.:
<http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html>



LEGAL PERSPECTIVE:

SEAN HOAR, PARTNER, LEWIS BRISBOIS
CHAIR OF THE DATA PRIVACY &
CYBERSECURITY PRACTICE

LEGAL PERSPECTIVE

HIPAA Security Rule

The HIPAA Security Rule requires covered entities and business associates to do the following, all of which are particularly important in preparing for an encryption attack:

- Implement a data backup plan as part of maintaining an overall contingency plan
- Conduct disaster recovery planning
- Conduct emergency operations planning
- Maintain an inventory of critical applications and data to ensure all are accounted for in the event of an emergency
- Periodic testing of contingency plans to ensure operational readiness

LEGAL PERSPECTIVE

The presumption of a breach

- Whether or not the presence of ransomware is a breach under the HIPAA Rules is a fact-specific determination.
- A breach under HIPAA is defined as, “...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI.”
- According to OCR guidance, when electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a “disclosure” not permitted under the HIPAA Privacy Rule.
- Unless the covered entity or business associate can demonstrate that there is a “...low probability that the PHI has been compromised,” based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred.

LEGAL PERSPECTIVE

The Importance of Forensics

Digital forensics investigations are a critical tool in conducting a breach risk assessment arising from a ransomware attack in the healthcare sector

A specific analysis pertaining to ransomware should be conducted in determine whether there is a low probability of compromise:

- the exact type and variant of malware discovered;
- the algorithmic steps undertaken by the malware;
- communications, including exfiltration attempts between the malware and attackers' command and control servers; and
- whether or not the malware propagated to other systems, potentially affecting additional sources of electronic PHI (ePHI).

Correctly identifying the malware will help determine its algorithmic behavior, and whether it is known to search for, view or acquire PHI, or whether it is known to drop other malicious code for future exploits



CYBER SECURITY PERSPECTIVE:

**BEN GOODMAN, PRESIDENT,
4A SECURITY & COMPLIANCE**

CYBER SECURITY PERSPECTIVE

WHY ARE SOME HEALTHCARE ORGANIZATIONS EASY TARGETS?

- Misconfigured security systems
- Vulnerable & unprotected systems (old and/or unpatched)
- No up-to-date threat feeds (zero days)
- Systems have admin privileges and admin tools
- No least privilege
- No web filtering (C2C)

CYBER SECURITY PERSPECTIVE

WHY ARE SOME HEALTHCARE ORGANIZATIONS EASY TARGETS?

- Weak server protection
- Weak credentials (RDP, etc.)
- No account lockout policies
- Unencrypted transport channels
- No network segmentation
- No data categorization

CYBER SECURITY PERSPECTIVE

WHAT TO PLAN FOR BEFORE RANSOMWARE STRIKES

- Extended down time procedures for being locked out of systems and data
- Determination re: unauthorized access of patient and other sensitive data
- Comprehensive planning (multiple down-time procedures, communications, leadership and coordination, etc.)
- Exercise the plan across the organization
- Train workforce (detection and response)
- Practice disaster recovery!

BEN GOODMAN

President, 4A Security & Compliance
goodmanb@4ASecurity.com
484-858-0427

SEAN HOAR

Partner, Lewis Brisbois,
Chair of the Data Privacy & Cybersecurity Practice
sean.hoar@lewisbrisbois.com

BARBARA HOLLAND

Regional Manager,
Health & Human Services, Office for Civil Rights
Barbara.Holland@hhs.gov

BEN STONE

Supervisory Special Agent, Cyber Desk, FBI

THANK YOU!

Thank you!

CLE Questions

CLE@LitigationConferences.com

HB Questions

Info@LitigationConferences.com

Tom.Hagy@LitigationConferences.com

(484) 324-2755

© Copyright HB Litigation Conferences LLC 2018