Ransomware:
Legal Issues and Practical Response

Romaine Marshall

Claire Rosston

HOLLAND&HART

Preliminaries

This presentation is similar to any other legal education materials designed to provide general information on pertinent legal topics. The statements made as part of the presentation are provided for educational purposes only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the speaker. This presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of law to your activities, you should seek the advice of your legal counsel.

Preliminaries

- Written materials:
  - .ppt slides
  - OCR Fact Sheet: Ransomware and HIPAA
  - US Interagency Guidance: How to Protect Your Networks from Ransomware
  - USDOJ Cybersecurity Unit: Best Practices for Victim Response and Reporting of Cyber Incidents
- Presentation will be recorded and available for download at www.hhhealthlawblog.com.
- If you have questions, please e-mail either of us at RCMarshall@hollandhart.com or CCRosston@hollandhart.com.

What Is Ransomware?

- Age-old crime with an electronic twist
  - Ransomware is malware that locks your computer or mobile devices or encrypts your electronic files.
  - Your data is held hostage until you pay the ransom to receive the decryption key. Some victims have paid ransoms and still been denied a decryption key.
  - Some ransomware also destroys or surreptitiously transfers your data.

HOLLAND&HART


CryptoLocker
CryptoLocker
Your important files encryption produced on this computer: photos, videos, documents, etc.
If you see this text, but do not see the "CryptoLocker" window, then your antivirus deleted "CryptoLocker" from computer.
If you need your files, you have to recover "CryptoLocker" from the antivirus quarantine, or find a copy of "CryptoLocker" in the Internet and start it again.
You can download "CryptoLocker" from the link given below.
http:// /1002.exe
Approximate destruction time of your private key:
11/13/2013 01:27 AM
If the time is finished you are unable to recover files anymore! Simply remove this wallpaper from your desktop.

In the News

- There has been a lot of media buzz around ransomware lately, particularly around two things:
  - Ransomware is on the rise.
  - The healthcare sector is under particular threat, with attacks increasing and of high consequence.
- Although healthcare organizations only account for a small percentage of ransomware victims, the fear is this percentage will grow as renegade hackers motivated by money turn their focus to the healthcare industry.

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

SC US
> SC UK

The SC UK Editorial Roundtable Series

VENDOR WEBCASTS
There will be attacks - Prepare your email defenses

NEWS | EVENTS | VIDEOS | JOBS | WHITE PAPERS | PRODUCTS

SC Magazine UK > News > Ransomware up 3000% since first recorded, now targeting hospitals

Roi Perez, Community Manager

Follow @scmagperez

September 14, 2016

Ransomware up 3000% since first recorded, now targeting hospitals

According to Intel Security the healthcare sector is under particular threat, with this industry experiencing over 20 data loss incidents per day.

HOLLAND&HART

Health Information Technology

Hospitals are hit with 88% of all ransomware attacks

Written by Max Green | July 27, 2016 | Print | Email

Hospitals and health systems have more to lose than organizations in other sectors when it comes to hacks. Patient data sells for more money than any other kind of information on the black market. Adding insult to injury, a new report suggests that the healthcare industry is hit significantly harder by ransomware than in any other — 88 percent of attacks hit hospitals.

NBC NEWS HOME TOP VIDEOS DECISION 2016 MORE

TECH › SECURITY

GADGETS INTERNET INNOVATION MOBILE

TECH MAR 23 2016, 5:16 PM ET

Three U.S. Hospitals Hit in String of Ransomware Attacks

by CONNOR MANNION

SHARE

Three U.S. hospitals were hit hard this week by "ransomware" attacks that brought down their systems — the latest providers of medical care to be targeted in this way.

HOLLAND&HART

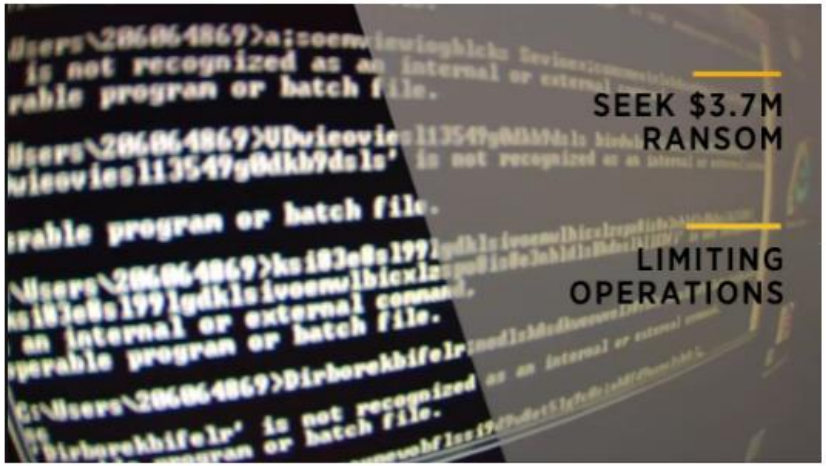
CYBERSECURITY

TECHNOLOGY | RE/CODE | MOBILE | SOCIAL MEDIA | ENTERPRISE | GAMING

The hospital held hostage by hackers

Anita Balakrishnan
15 Hours Ago

CNBC



Los Angeles medical workers are dealing with an internal emergency straight out of science fiction, one that cybersecurity experts say is increasingly common.

CNBC (February 17, 2016)

- Hollywood Presbyterian Hospital hit by ransomware.
- Medical record system shut down.
- Hackers demand $3.7 mil in bitcoin.

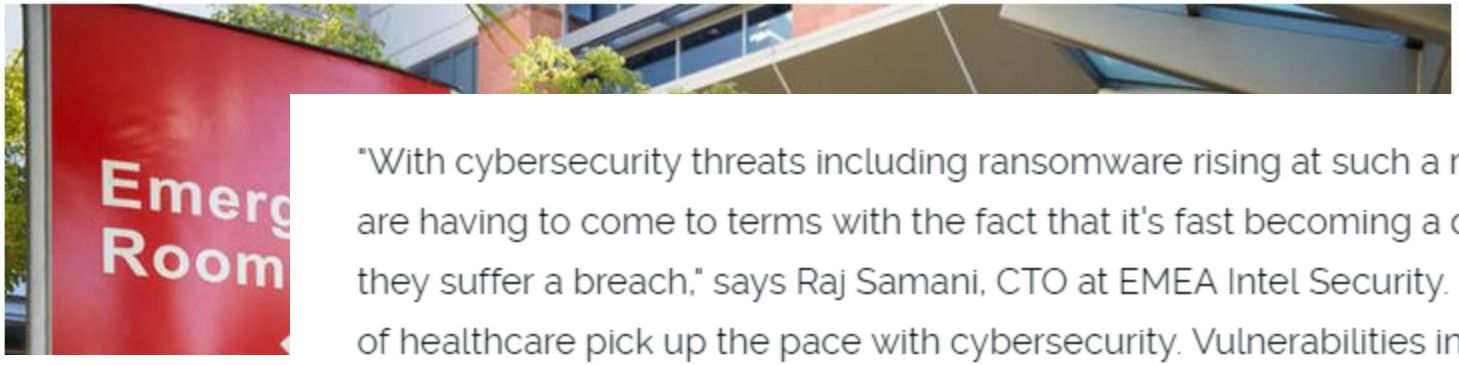
ZDNet MENU US

MUST READ FOR PRIVACY AND SECURITY, CHANGE THESE IOS 10 SETTINGS RIGHT NOW

Hackers split on 'ethics' of ransomware attacks on hospitals

Ransomware might be lucrative for some cybercriminals, but there are those who condemn holding hospitals to ransom.

By Danny Palmer | September 14, 2016 -- 07:55 GMT (00:55 PDT) | Topic: Security



"With cybersecurity threats including ransomware rising at such a rapid rate, organisations are having to come to terms with the fact that it's fast becoming a question of 'when', not 'if', they suffer a breach," says Raj Samani, CTO at EMEA Intel Security. "It's crucial that the likes of healthcare pick up the pace with cybersecurity. Vulnerabilities in these sectors provide hackers with access to extremely personal, valuable and often irreplaceable data and IP."

HOLLAND&HART

Why Is Healthcare a Target?

- Show me the MONEY!!!
  - Ransom payments
  - Selling the EHR on the black market
- Weak security of legacy systems and medical devices, creating many easy points of entry

Significant Costs

Direct Costs	Indirect Costs
Ransom payment	Lost productivity
Lost revenue during downtime	Temporary loss of revenue from follow-up services stemming from patients going elsewhere during downtime
System recovery costs	Damage to reputation (patients go elsewhere permanently)
Incident response, including breach notification and mitigating breaches (e.g., credit monitoring)	
Audit services	

Government Response and Guidance

- FBI – Published resources about ransomware and how to deal with it
- FTC – Held seminar on ransomware on September 7, 2016, announcing: (1) it will soon offer guidance on how businesses can protect themselves against ransomware and (2) its primary method of protecting U.S. consumers' privacy will be through enforcement
  - Federal Trade Comm'n Act ("FTCA") § 5 (15 USC 45(a)): Prohibits unfair (inadequate security measures) or deceptive (misrepresentations re privacy policy) acts affecting commerce

LabMD, Inc., In the Matter of

TAGS: Health Care | Consumer Protection | Privacy and Security | Data Security

LAST UPDATED: FEBRUARY 5, 2016

In the Matter of LabMD, Inc., a corporation

FTC MATTER/FILE NUMBER: 102 3099

DOCKET NUMBER: 9357

RELATED CASE: LabMD, Inc. v. Federal Trade Commission

CASE SUMMARY

The Federal Trade Commission filed a complaint against medical testing laboratory LabMD, Inc. alleging that the company failed to reasonably protect the security of consumers' personal data, including medical information. The complaint alleges that in two separate incidents, LabMD collectively exposed the personal information of approximately 10,000 consumers. The complaint alleges that LabMD billing information for over 9,000 consumers was found on a peer-to-peer (P2P) file-sharing network and then, in 2012, LabMD documents containing sensitive personal information of at least 500 consumers were found in the hands of identity thieves. The case is part of an ongoing effort by the Commission to ensure that companies take reasonable and appropriate measures to protect consumers' personal data.

Government Response and Guidance

- HHS
  - June 20, 2016 letter to healthcare organizations on the increasing threat of ransomware
- OCR
  - July 11, 2016 guidance on ransomware

OCR Guidance

- Confirms ransomware attacks = security incidents
- Therefore, you must initiate your security incident response and reporting procedures upon detection of the attack, which require you to:
  - **Analyze** the scope, origin, status, and methodology of the ransomware
  - **Isolate** the infection and **preserve** evidence
  - **Recover** (restore data from backups or pay ransom and hope your files are unlocked)
  - **Report** to affected individuals, HHS Secretary, and the media (for breaches of >500 only)

OCR Guidance: Reporting Exceptions

- Low Risk of Compromise
  - If you can document there is a low probability of compromise of the data that was encrypted by the ransomware, there is no reporting obligation under the HIPAA breach notification rule.
  - This requires a thorough risk assessment completed in good faith.
- Encrypted PHI

Response: Pre-attack

- Keep system patches up to date or application whitelist, use a firewall, and disable unnecessary services or ports
- Use antispam
- Network segmentation
- “Air gap” backups
- User-awareness education
- Cyber incident response plan

Response: During Attack

- Step 1: Assess and Preserve Evidence
- Step 2: Implement Measures to Minimize Continuing Damage
- Step 3: Record and Collect Information
- Step 4: Notify

Additional Resources

www.hollandhart.com/cyber-security

w.hollandhart.com/cyber-security

HOLLAND&HART

search this site

people
practices
firm
locations
news & resources
blogs
community

Contact
Disclaimer
Site Map

- Review existing cyber insurance and advise on recommended policy features and coverage levels.

When a breach occurs, we quickly mobilize to efficiently help businesses and organizations:

- Identify data breach root cause and incident containment
- Guide IT staff during initial incident triage and data breach investigation.
- Oversee and coordinate the work of digital forensics, public relations, and data breach consultants.
- Comply with all applicable breach notification laws

To protect and defend your company or organization against data breaches, contact one of our experienced team members.

– Publications

The Rising Cost of Ransomware Attacks: Add Breach Notification Expenses Per HHS Guidance

Holland & Hart News Update
Author(s): **Claire Rosston**, and **C. Matt Sorensen**

Waiting May Cost You: Sanctions for Inadequate Cybersecurity Practices May Be Imposed Before a Cyber Attack

Holland & Hart News Update
Author(s): **Romaine Marshall**, and **Engels Tejeda**

Protect Yourself and Your Company From Ransomware

Holland & Hart News Update
Author(s): **C. Matt Sorensen**

Third Circuit Finds that the FTC Has Authority to Sue Companies for Inadequate Cybersecurity Practices as an "Unfair" Practice

Holland & Hart News Update
Author(s): **Romaine Marshall**
Co-author(s): Geoff Barry

Additional Resources

- www.nomoreransom.org
- Matt Sorensen, Post-Breach Response, available at https://www.hollandhart.com/pdf/Post_Breach_Response.pdf
- Kim Stanger, Responding to HIPAA Breaches (November 6, 2015), available at https://www.hollandhart.com/responding-to-hipaa-breaches
- McAfee Labs, Threat Report (September 2016), available at www.mcafee.com/uk/resources/reports/rp-quarterly-threats-sep-2016.pdf

Future Webinars

- *Health Law Basics* monthly webinar series
  - 9/22/16 Medical Records
  - 9/29/16 Marketing Traps for Providers
  - 10/13/16 Antitrust Issues in Healthcare
  - 10/27/16 Handling Problem Patients
- *Healthcare Update* and *Health Law Blog*
  - Under "Publications" at www.hollandhart.com.
  - E-mail kcstanger@hollandhart.com.

Questions?

Romaine Marshall

Holland & Hart LLP

rcmarshall@hollandhart.com

801-799-5922

Claire Rosston

Holland & Hart LLP

ccrosston@hollandhart.com

208-383-3960