Your Money or Your PHI: Ransomware in the Healthcare Industry

Arizona Society for Healthcare Risk Management

November 11, 2016
AGENDA

- What is Ransomware?
- Why are We Talking About it Today?
- What's at Stake?
  - Patient Health & Safety
  - Regulatory Compliance
    - HIPAA & State
    - Breach Notification
  - Financial Losses
  - Your Reputation
- Insurance Coverage for Cyber / Ransomware Attacks
- Recommendations
RANSOMWARE 101

Ransomware is a type of malware (malicious + software) that encrypts a victim’s files, locking users out of the infected device/system or blocking access to encrypted files.

In order to acquire the key to decrypt these files, the victim must pay a ransom, often in the form of bitcoin or other electronic currency.
• Ransomware typically sent as an email attachment or an embedded code / link in a webpage or email
• Emails historically generic (phising); increasingly targeted to specific individual (spear phising)

(1) source

(2) infection

• Once opened or clicked, ransomware begins encrypting all available files, without user interaction or notification
• If user’s machine is connected, available files can include files on network, cloud, shared services, etc.

(3) ransom notice

• Once encryption is complete, ransomware alerts the user of infection, blocks access to system / files and provides payment instructions for decryption key

(4) pay or ???

• Key choice:
  - Pay ransom; or
  - Restore from backup
Cybercriminals don’t need to be “high-tech” or particularly tech savvy. All of the tools they require are available at reasonable cost.¹

“Ransomware-as-a-Service” is readily available and cheap and in some instances for free.²

A phishing page and a mass spam email to deliver the Ransomware can be purchased in an off-the-shelf malware for about $150.¹

---

RANSOMWARE IS PROFITABLE

- Established business case for Ransomware
  - Ransomware will net criminals $1B (est.) in 2016.¹
  - High-end Ransomware costs about $2k through dark net forums²; the average ransom demand is $679³.
  - An attacker needs to ransom four “normal” (individual) users (or one hospital / enterprise with mission-critical data) to generate a profit.

². Institute for Critical Infrastructure Technology, ICIT Ransomware Report: 2016 Will Be the Year Ransomware Holds America Hostage.
RANSOMWARE IS PROFITABLE

How hackers earn money

User’s losses

Money from bank accounts

$722

Money for data decryption

$100-200

Paying to unblock the OS

$10-200

Photos, contacts, personal correspondence

Priceless

Cybercriminal profits*

Banking Trojan
Exploit
Spam mass mailing

$3000

Encryption ransomware
Exploit
Renting a botnet
Spam mass mailing

$20 000

Mobile Trojan blocker
Placing the application in Google Play

$1000

Phishing page on a social network
Renting hosting
Spam mass mailing

$10 000

$20 000

©2014 Kaspersky Lab
“You don’t want to think of return on investment as it pertains to criminal activity, but there is a strong ROI, and these attackers are quite sophisticated and know there is money to be made.” Elliott Frantz – CEO of Virtue Security

The payoff for hackers can be huge. The FBI estimated in 2014 that the extortionists behind the CryptoLocker strain of ransomware swindled some $27 million in just six months out of people whose data they took hostage.
 Fill your shopping cart and you’re off
RANSOMWARE 101

A video summary:

Source: ESET [IT security company]
Why Are We Talking About Ransomware TODAY?
### Healthcare is Big and Vulnerable

<table>
<thead>
<tr>
<th>Giant Industry</th>
<th>Technology Dependent</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 5,627 U.S. Hospitals (AHA 2016 Report)</td>
<td>• Digital Health Records</td>
</tr>
<tr>
<td>• 35M hospital admissions per year + &gt;100M outpatient encounters at doctor offices, hospital outpatient departments, pharmacies, behavioral health centers, etc. → innumerable patient records and data</td>
<td>• 90% of hospitals implemented EHR</td>
</tr>
<tr>
<td>• Healthcare records are 10 times more valuable on the black market than credit cards</td>
<td>• Health Information Exchange driving further digitization and connectedness</td>
</tr>
<tr>
<td></td>
<td>• Delivery of care requires sophisticated technology (diagnostics, bedside point of care systems, etc.)</td>
</tr>
<tr>
<td></td>
<td>• Wellness and prevention efforts technology dependent (distance care, wearables, implanted devices)</td>
</tr>
</tbody>
</table>
**Healthcare is Big and Vulnerable**

| **Rapid Change and Consolidation** | **Unprecedented industry consolidation**  
| | • Complex networks (patchworks) of “legacy” systems  
| | • Provide a collaborative, transparent, and real-time platform to deliver service regardless of where the expertise may lie  
| **High Touch** | **Staff intensive (most of whom have access to EHR and financial systems)**  
| | • Staff splitting time between facilities requires access across multiple systems  
| | • Many non-employees permitted access (e.g., medical staff)  
| **Immature Cybersecurity** | **Outdated approaches, frequently failing at securing organizations from today’s increasingly sophisticated cybercriminals**  
| | • 2 major IT security issues: HIPAA-centric focus (defending patient records) and security measures defending against yesterday’s issues  

**HACKERS LOVE HEALTHCARE**

---

*November 11, 2016*  
*©2016 Integro Insurance Brokers*
HEALTHCARE IS A TARGET

HACKING HEALTHCARE
Cybercriminals Find Value in Holding Data Hostage As Alternative to Putting it Up For Sale
FLASHPOINT
HEALTHCARE RANSOMWARE TRENDS

- According to the FBI, Ransomware has quickly become one of the larger threats to healthcare cyber security.¹
- At least 14 hospitals have been attacked by ransomware in 2016.²
- Healthcare data breaches are frequent and impact everyone:
  - Nearly 90% of hospitals reported a data breach in the past 2 years; 45% had 6 or more data breaches.³
  - About 47% of US population has had their personal healthcare data compromised over last 12 months.³

WHY IS HEALTHCARE A TARGET FOR RANSOMWARE

“Hospitals are the perfect mark for this kind of extortion. [They] are more likely to pay a ransom rather than risk delays that could result in death and lawsuits.”¹

- Staggering amounts of valuable electronic data, which is not required to be encrypted “at rest”.
- Reliant on technology to deliver patient care.
- Increasing connectivity of care and interconnectivity of healthcare industry.
- Tremendous number of access points for criminals (systems and users).
- Insecure and antiquated networks vulnerable to attacks.²

“It's very common for hospitals to have a large number of outdated and vulnerable systems on the network.”

CASE STUDIES: 5 RECENT RANSOMWARE ATTACKS

- MedStar Health
- Kansas Heart Hospital
- Christopher Rural Health
- Methodist Hospital (KY)
- Hollywood Presbyterian Medical Center

![MedStar Health Image](image-url)
Ransomware – What’s at Stake for Healthcare Companies?
WHAT’S AT STAKE

- **Patient Health & Safety**
  - Loss of EHR access can impede the ability to treat patients.
  - Lack of control over essential medical equipment can endanger patients.

- **Regulatory Compliance**
  - Ransomware (or any malware) on a covered entity’s or business associate’s systems is a HIPAA security incident.¹
  - Ransomware attack involving protected health information is presumptively a HIPAA Breach.¹
  - State data security and breach reporting laws may also be implicated.

---

WHAT’S AT STAKE

▪ Financial Implications
  ▪ Ransom payment
  ▪ Business Interruption and Extra Expense
  ▪ Incident response, legal, forensic IT, etc. expenses
  ▪ Data restoration costs
  ▪ Regulatory expenses – defense & fines (e.g., DHHS fines for HIPAA violations and associated defense costs)
  ▪ Patient lawsuits
  ▪ Notification expenses

“The potential for corporate losses from cyber attacks goes far beyond downtime and lost revenue… If attacks delay the release of medicines to patients[, render inoperable or accessible EHR systems, or shut down critical medical equipment, they can endanger lives and result in punitive damages.” Fiona Barry – Ex-Homeland Security Cyber Chief

▪ Reputational Risk
  ▪ “The reputational hit [from a breach]… could be an extinction-level event.” Vincent Polley – Co-Author of American Bar Association Cyber-Security Handbook
PER RECORD COST BY INDUSTRY CLASS

Healthcare: $363
Education: $300
Pharmaceutical: $220
Financial: $215
Communications: $179
Retail: $165
Industrial: $155
Services: $137
Consumer: $136
Energy: $132
Hospitality: $129
Technology: $127
Media: $126
Research: $124
Transportation: $121
Public Sector: $68

Source: Ponemon 2015 Cost of Data Breach Study
Cyber Insurance
CYBER RISKS COVERED BY NON-CYBER POLICIES?

- CGL/HPL/D&O Policies may provide a very limited amount of coverage for cyber events, but they do not provide adequate coverage
  - Potential for some overlap in coverage
  - Cyber exclusions
  - Underwriting intent?
  - Regulatory Defense/Fines & Penalties
  - First Party Coverage is crucial
  - Pre-Breach Risk Mitigation Services
  - Post-Breach Response Services
BASIC CYBER COVERAGES

- **Third Party (Liability) Coverages**
  - Security & Privacy Liability
  - Notification Expenses and Response Services
  - Regulatory Defense & Indemnity
  - Media Liability

- **First Party Coverages**
  - Cyber Extortion/Ransomware/Cyber Terrorism/Cyber Theft
  - Network/Business Interruption
  - Contingent Network/Business Interruption
  - Data Recovery & Restoration
  - Public Relations/Crisis Management
  - Forensic Investigation

- **Risk Management**
  - Pre-Breach Risk Mitigation Services
  - Breach Response Services
# Key Exclusions to Review

## Third party acts/omissions
- Some policy forms do not respond to breaches of/attacks against third-parties’ networks. Need to ensure your policy will respond if your data, especially PHI, is stored/maintained by third parties (cloud services, EHR vendors, shared services, etc.) is breached.
- “Shaving of limits” – essential for policy to recognize indemnity payments from third parties.

## Off-site Security Failures
- Some policy forms limit some coverages to losses occurring from your premises. Do your employees bring devices or equipment with PHI (laptops, phones, external drives, etc.) off site?

## Terrorism / War
- Escalation of cyber terrorism and state-sponsored attacks create potential coverage issues. Attempt to have these removed.

## IT Security Deficiencies
- IT Security Warranty – policy holder warrants IT security is maintained to the same level as represented in policy application. The dynamic nature of IT generally and the number of legacy and ancillary systems can potentially lead to lack of coverage clarity.
- Certain policy forms exclude coverage for incidents caused by failure to maintain and update IT security software and features. So ex post facto hypothesizing invites disputes.
<table>
<thead>
<tr>
<th>Policy Terms to Review</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prior Acts Coverage</strong></td>
</tr>
<tr>
<td>• New (v. renewal) policies typically limit coverage to events occurring after policy inception. Undetected but ongoing attacks at inception are not covered unless this condition is limited.</td>
</tr>
<tr>
<td>• Knowledge requirements should be limited to appropriate executive team members (e.g., Legal, IT and RM).</td>
</tr>
<tr>
<td><strong>Continuity of Coverage</strong></td>
</tr>
<tr>
<td>• Do <strong>NOT</strong> sign warranties related to circumstances or claims when renewing coverage.</td>
</tr>
<tr>
<td><strong>Panel Vendors</strong></td>
</tr>
<tr>
<td>• If you have a preferred vendor (IT consulting / forensics, legal, etc.) that is not on your insurer’s panel list, seek the approval to use such vendors early and well before a breach.</td>
</tr>
<tr>
<td><strong>Notice Issues</strong></td>
</tr>
<tr>
<td>• Look for permissible delay in reporting due to non-disclosure recommendation by law enforcement (FBI).</td>
</tr>
<tr>
<td><strong>Defense Trigger</strong></td>
</tr>
<tr>
<td>• Defense coverage under some policies triggered by “suits”. This limits coverage for matters that have not yet developed into litigation. Coverage for pre-“suits” (investigative demands, etc.) especially important for regulatory coverage.</td>
</tr>
</tbody>
</table>
Some Recommendations
PRE-INCIDENT CONSIDERATIONS

- **Assemble the Team**
  - Internal – RM, IT, Legal
  - External – Legal, PR, Broker/Insurer

- **Identify the Risk**
  - ERM Basics: What kind of data you have: How much? Where is it? Why do you have it? Who has it? Who gets to see it?
  - What vendors and other 3rd parties have access?

- **Elevate the Issue**
  - Board education and involvement is critical

- **Cyber Incident Response Plan**
  - Is it stale?
  - Outside expert review?
  - HIPAA Compliance
HIPAA PLANNING REQUIREMENTS

“Organizations need to take steps to safeguard their data from ransomware attacks. HIPAA covered entities and business associates are required to develop and implement security incident procedures and response and reporting processes that are reasonable and appropriate to respond to malware and other security incidents.”

Jocelyn Samuels – Director U.S. Department of Health & Human Services, Office of Civil Rights
PRE-INCIDENT CONSIDERATIONS

- Business Continuity Plan
- Table Top Exercises (fire drills)
- Education, Education, Education
- Vendor Contracts / Issues
  - Data security responsibility and requirements
  - Indemnity for breaches
  - Breach notification requirements
- Insurance
  - Funding mechanism; not a substitute for preventive measures and pre-loss planning
  - Does your coverage match your exposure?
  - Meet and use panel vendors before a loss
- IT Cybersecurity
  - Identifying who owns it and working to ensure this remains a priority.
POST-INCIDENT CONSIDERATIONS

- Assemble and Inform the Team
  - Internal – RM, IT, Legal
  - External – Legal, PR, Broker/Insurer
- Pull Cyber Incident Response Plan
- Notify cyber insurer(s)
- Isolate the infected equipment
- Data recovery / restoration
- Pay the ransom?
- Breach notification and HIPAA considerations
  - Get qualified legal counsel involved immediately. Relatively short windows under some laws.
- Post-Mortem / Remediation
Contact: John Selgrath
(415) 365-4675
John.Selgrath@integrogroup.com