THE GROWING CYBERSECURITY THREATS IN TELEMEDICINE
Industry Accomplishments
What is Hacking?

- **Hacking**
  - Method in which one bypasses or modifies the normal operation of a system
    - Exploits
    - Vulnerabilities
The Business of Hacking

- Purpose in the early day’s
  - Pride
  - Glory

- Today’s purpose
  - Profits
  - Espionage
  - Hacktivism
Types of Cybersecurity Attacks

- Attack vectors
  - Phishing
  - Social Engineering
  - Malware/Ransomware
  - Denials of Service (DoS)
  - Session Hijacking & Man-in-the-Middle
Where Does Healthcare Fit?

- #1
  - Highest number of data breaches

**Number of Data Breaches by Industry in 2014**

- Healthcare: 42%
- Business: 33%
- Government: 12%
- Other: 13%

Source: fluiddesigns.org
Reasons to Attack Healthcare

- 2016 Healthcare Information and Management Systems Society (HIMSS) Study
  - Medical Identity Theft
    - #1 Concern
      - 77% of respondents
  - Black Market/Organized Crime
- Over 113.2 million healthcare records stolen in 2015
Health Records

- Where is the value?
  - Electronic Health Record
    - Demographics
    - Insurance Information
    - Mailing Address
    - Social Security Number
    - Birthdate
    - Medication
    - Billing Information
      - Credit Card Numbers
Value in Health Records

- EHR = PII + Medical History + Insurance + Financial
  - This unique combination differentiates healthcare hacks from other industries
Value in Health Records

- Personal Identifiable Information (PII)
  - No Expiration Date = Greater Value
    - Name
    - Date of Birth
    - Social Security Number
Value in Health Records

- Uses
  - Obtain pharmaceuticals
  - Commit insurance fraud
  - Obtain medical care
    - Medicare
    - Medicaid
Health Records Sold on Darkweb

Stolen Health Record Databases Sell For $500,000 In The Deep Web

Electronic health record databases proving to be some of the most lucrative stolen data sets in cybercrime underground.

Medical insurance identification, medical profiles, and even complete electronic health record (EHR) databases have attracted the eyes of enterprising black hats, who increasingly see EHR-related documents as some of the hottest commodities peddled in the criminal underground. A new report today shows that complete EHR databases can fetch as much as $500,000 on the Deep Web, and attackers are also making their money off of smaller caches of farmed medical identities, medical insurance ID card information, and personal medical profiles.

The data comes by way of a report from Trend Micro’s TrendLabs Forward-Looking Threat Research (FTR) Team, which took a comprehensive look at how attackers are taking advantage of healthcare organizations’ weaknesses to devastating effect. Cybercriminals always have their eyes open for new profitable revenue streams, and the poor security around increasingly data-rich EHR systems pose a huge opportunity for the bad guys.
Health Records Sold on Darkweb

Medical clinic records for sale (1 hand only) 5200 records Minnesota USA !!!

Hacked clinic details !!! Medical clinic records for sale (1 hand only) 5200 records Minnesota USA !!! Details sample: Patient First Name; Patient Middle Name; Patient Last Name; Patient Address1; Patient Address2; Patient City; Patient State; Patient Zip Code; Home Phone; Date Of Birth; Patient SSN; Patient Sex

Sold by trtter - 0 sold since Feb 27, 2017

Vendor Level 3 Trust Level 6

<table>
<thead>
<tr>
<th>Features</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product class</td>
<td>Digital goods</td>
</tr>
<tr>
<td>Quantity left</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Ends in</td>
<td>Never</td>
</tr>
<tr>
<td>Origin country</td>
<td>Worldwide</td>
</tr>
<tr>
<td>Ships to</td>
<td>Worldwide</td>
</tr>
<tr>
<td>Payment</td>
<td>Escrow</td>
</tr>
</tbody>
</table>

Default - 1 days - USD +0.00 / item

Purchase price: USD 99.00

Qty: 1
Buy Now

Product Description

Hacked clinic details !!!

Medical clinic records for sale (1 hand only) 5200 records Minnesota USA !!!
How Prevalent?

- Bitglass’ Healthcare Breach Report
  - 1 in 3 Americans victims of healthcare data breaches
Consequences for You

- Department of Health and Human Services’ Office for Civil Rights (OCR)
  - Fines
- Loss of consumer trust
- Loss of consumer confidence
- Loss of patient to competing provider
- Reporting, analysis, review and remediation costs
HIPAA

- Department of Health and Human Services’ OCR
  - Enforcing rules
  - 2016
    - 13 settlements
    - $22.8 million in payments
## Cost of HIPAA Violations

<table>
<thead>
<tr>
<th>Covered Entity</th>
<th>Amount</th>
<th>Date</th>
<th>Breach that triggered OCR investigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>University Medical Center</td>
<td>$650,000</td>
<td>11/2016</td>
<td>Malware infection</td>
</tr>
<tr>
<td>Health System</td>
<td>$2,140,500</td>
<td>10/2016</td>
<td>PHI made available through search engines</td>
</tr>
<tr>
<td>Health System</td>
<td>$400,000</td>
<td>9/2016</td>
<td>Loss of two unencrypted backup tapes</td>
</tr>
<tr>
<td>Health System</td>
<td>$5,550,000</td>
<td>8/2016</td>
<td>Theft of desktop computers, loss of laptop, improper access of data at business associate</td>
</tr>
<tr>
<td>University Medical Center</td>
<td>$2,750,000</td>
<td>7/2016</td>
<td>Unprotected network drive</td>
</tr>
</tbody>
</table>
## Cost of HIPAA Violations

<table>
<thead>
<tr>
<th>Covered Entity</th>
<th>Amount</th>
<th>Date</th>
<th>Breach that triggered OCR investigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Associate</td>
<td>$650,000</td>
<td>6/2016</td>
<td>Theft of mobile device</td>
</tr>
<tr>
<td>Hospital</td>
<td>$2,200,000</td>
<td>5/2016</td>
<td>Filming of patients by TV crew</td>
</tr>
<tr>
<td>Physician Group</td>
<td>$750,000</td>
<td>4/2016</td>
<td>Improper disclosure to business associate</td>
</tr>
<tr>
<td>Medical Research</td>
<td>$3,900,000</td>
<td>3/2016</td>
<td>Improper disclosure of research participants’ PHI</td>
</tr>
<tr>
<td>Institute</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Health System</td>
<td>$1,550,000</td>
<td>3/2016</td>
<td>Theft of laptop computer / Improper disclosure to business associate (discovered during investigation)</td>
</tr>
</tbody>
</table>
# Cost of HIPAA Violations

<table>
<thead>
<tr>
<th>Covered Entity</th>
<th>Amount</th>
<th>Date</th>
<th>Breach that triggered OCR investigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Therapy Provider</td>
<td>$25,000</td>
<td>2/2016</td>
<td>Improper disclosure of PHI (website testimonials)</td>
</tr>
<tr>
<td>Infusion and Equipment Provider</td>
<td>$239,800</td>
<td>2/2016</td>
<td>Improper disclosure (unprotected documents)</td>
</tr>
</tbody>
</table>

*Data Source: U.S. Department of Health and Human Services Office for Civil Rights*
Protecting Patient Data

- Protecting patient data = protecting yourself
Protecting Patient Data

- Third Party Audits
- Vulnerability Testing
- Penetration Testing
- Hardware Solutions
  - Firewalls
    - Unified Threat Management (UTM) Firewalls
    - Next-Gen Firewalls (NGFW)
Protecting Patient Data

- Software Based Solutions
  - Encryption
  - Antivirus
  - Antimalware
  - E-mail Spam Filtering
  - Application Containerization
    - Work Container
    - Personal Container
  - Data Backup
Protecting Patient Data

- User Education
  - Do not share passwords
  - Enable two-factor authentication
  - Do not use third party device
    - Ex: Free USB flash drive
  - Do not open e-mails and/or attachments from unidentified individuals
  - Do not allow a random person who calls access to your computer/device
Remote Worker Protections

- **Mobile Device Protection**
  - Never leave devices unattended
  - Lock devices if unattended
  - Avoid logging to secure sites or portals around people
  - Do not use public wireless hotspots
Breach

What to do?

- Follow protocol
- Shutdown All Systems
- Contact your IT provider or department
Stanley Louissaint
Principal and Founder, Fluid Designs
- Managed Service Provider
- Computer and Network Support/Consulting
- Cybersecurity Penetration Testing
- Business Continuity Solutions
- e-Discovery & Litigation Support

908-688-2444
www.FluidDesigns.com
www.LinkedIn.com/in/slouissaint
slouissaint@fluiddesigns.com
Questions?

Thank You!