Healthcare Data Breaches – Is There A Cure?

Josephine Bottitta
Esq.
OneGroup

Dennis Ast
CPCU, CCIC
OneGroup

Dennis O’Connell
Director
Custom Computer Specialists
FBI Internet Crime Complaint Center (IC3)

- 2019 1,300/day grew to 4,000/day in 2020
- $4.2 Billion in losses
- Email is the most common entry point
- Smishing (text messages)
- Pharming (fake websites)
- Vishing (phone calls or messages)
- Attacks are “more targeted and sophisticated”
- Attacks are more costly
IC3 Crimes by Victim Count

<table>
<thead>
<tr>
<th>Crime Type</th>
<th>Victims</th>
<th>Crime Type</th>
<th>Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing/Vishing/Smishing/Pharming</td>
<td>241,342</td>
<td>Other</td>
<td>10,372</td>
</tr>
<tr>
<td>Non-Payment/Non-Delivery</td>
<td>108,869</td>
<td>Investment</td>
<td>8,788</td>
</tr>
<tr>
<td>Extortion</td>
<td>76,741</td>
<td>Lottery/Sweepstakes/Inheritance</td>
<td>8,501</td>
</tr>
<tr>
<td>Personal Data Breach</td>
<td>45,330</td>
<td>IPR/Copyright and Counterfeit</td>
<td>4,213</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>43,330</td>
<td>Crimes Against Children</td>
<td>3,202</td>
</tr>
<tr>
<td>Spoofing</td>
<td>28,218</td>
<td>Corporate Data Breach</td>
<td>2,794</td>
</tr>
<tr>
<td>Misrepresentation</td>
<td>24,276</td>
<td>Ransomware</td>
<td>2,474</td>
</tr>
<tr>
<td>Confidence Fraud/Romance</td>
<td>23,751</td>
<td>Denial of Service/TDoS</td>
<td>2,018</td>
</tr>
<tr>
<td>Harassment/Threats of Violence</td>
<td>20,604</td>
<td>Malware/Scareware/Virus</td>
<td>1,423</td>
</tr>
<tr>
<td>BEC/EAC</td>
<td>19,369</td>
<td>Health Care Related</td>
<td>1,383</td>
</tr>
<tr>
<td>Credit Card Fraud</td>
<td>17,614</td>
<td>Civil Matter</td>
<td>968</td>
</tr>
<tr>
<td>Employment</td>
<td>16,879</td>
<td>Re-shipping</td>
<td>883</td>
</tr>
<tr>
<td>Tech Support</td>
<td>15,421</td>
<td>Charity</td>
<td>659</td>
</tr>
<tr>
<td>Real Estate/Rental</td>
<td>13,638</td>
<td>Gambling</td>
<td>391</td>
</tr>
<tr>
<td>Advanced Fee</td>
<td>13,020</td>
<td>Terrorism</td>
<td>65</td>
</tr>
<tr>
<td>Government Impersonation</td>
<td>12,827</td>
<td>Hacktivist</td>
<td>52</td>
</tr>
<tr>
<td>Overpayment</td>
<td>10,988</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Are We Witnessing a Cyber Pandemic?

- New York Pause March 22nd
  - IT began enabling employees to work at home as quickly as possible
  - Schools started distance learning

- Attack surface expanded exponentially
  - No firewalls at home
  - Access was grants without adequate controls
  - “Employee owned” computers given access
  - No way to verify users
  - Education was lacking

- Hackers took notice
  - They only need control of 1 computer
  - Phishing up 98%
  - Increase in user and network compromised
Healthcare is the Second most Targeted Industry
2020 – Healthcare Breaches (Sept-Oct)

- 5,000 Computers for 40 days
- Reassigned or furloughed 300 workers
- $1.5M/day loss
- 6 Hospitals in a 24-hour period
- 400 more targeted
- Rapid tightening of security controls
- 26 Hospitals, hundreds of facilities
- 8 days on paper

- EHR and Patient Portal Access
- 219K records stolen
- Other Hospitals impacted

- Initially reported no significant data loss
- SEC filing revealed more than thought
- 46 Hospitals had data exposed

• Weeks
  • New York Pause – Initial Compromise
  • Reconnaissance
  • Exploit weakness for Lateral movement
  • Privilege Escalation

• Months
  • Gain Control
  • Build Attack
  • Attack and Cover
Common Attack Vectors

Types of cyber security attacks:

- Cross-Site Scripting (XSS)
- Phishing Attack
- DoS/DDoS
- Vishing Attack
- Viruses
- Malware Attack
- Brute Force Attack
- Spyware and Keyloggers
- Password Attacks
- Man-in-the-Middle Attack
- SQL Injection Attack
Why the Industry is Under Attack

• Easy Targets
  • Movement to digital records without adequate protection
  • Proliferation of attached devices
    • MoIT
    • IoT
    • Cloud/Hosted
    • Vendor Supplied
  • Most organizations are unprepared for an “Event”

• The Money
  • The Value of Medical Records
  • Ransomware
My Organization is Not a Target!

- Department of Homeland Security
  - 50%-70% of all Ransomware Attacks target SMB’s
  - 300% increase in 2020

- Verizon 2020 Data Breach Report
  - 28% of all Cyber Breaches occurred at small business
  - Organized Crime account for 55% of the breaches
  - Internal Actors 30%

- IBM 2020 Cost of a Breach Report
  - Average cost of a breach globally $3.86m
  - Healthcare data breach is costliest at $7.13m up 10.5% year over year
  - Healthcare breach take on average 186 days to identify and 51 days to contain an attack
What is the Impact of a Breach to Your Organization

Approximately $254 per Record

- Direct Remediation
  - Systems Repair
  - Employee Costs
- Indirect Costs
  - Regulatory or Industry Fines
  - Civil Lawsuits
  - Higher Cyber Premiums
  - Customer Refunds and Incentives (Credit Monitoring)
  - Systems Down Time
- Ongoing Costs
  - Systems Improvement
  - Auditing and Reporting
  - Reputation – Lost Sales and Business Opportunities
What Can You Do!

• Develop a Security Program

• Educate Your Staff

• Prepare for the Worst

• Implement Appropriate Technical Safeguards

• Test and Inspect
Develop a Security Program & Adopt a Framework

- Frameworks
  - National Institute of Standards and Technology (NIST)
  - Health Information Trust Alliance (HiTrust)
  - Payment Card Industry (PCI)
- Implement, Measure, and Refine
  - Internal
  - Business Associates
Educate Your Staff

• Common Threats
• Cyber Security Awareness
• Policies and Procedures
• Email Safety
• Safe Web Browsing
• Handling Sensitive Information
• Mobile Device Security
• Open WiFi Security
• Credit Card Security
• Strong Passwords
Prepare for the Worst

• Risk Assessment

• Reassess Cyber Insurance
  • Conditions
  • Limits
  • Exclusions

• Incident Response Planning and Testing
Prepare for the Worst Case

Quantify the Risk (Risk Assessment)

- People
  - Staff
  - 3rd Party/Business Associates
- Technologies
  - EMR & Other Applications
  - On Premise
  - Cloud
  - Mobile
  - MoT/IoT
- Business
  - Acceptable Down Time and Time to Restore
  - How often is Assessment done
Prepare for the Worst Case

Cyber Insurance

• Reassess Cyber Insurance Coverage
  • Conditions
  • Limits
  • Exclusions
Prepare for the Worst Case

*Incident Response Planning*

- Develop Playbooks
  - Ransomware
  - Malicious Insider
- How will you know
- What should you do! What shouldn’t you do!
- What are your Priorities
  - Who do you call first
  - What order do systems need to come back on
  - Do you have a working backup and can you restore
- What notifications need to be made
- How do you prevent/minimize in the future
Prepare for the Worst Case  
*Incident Response Testing/Simulation*

**Setting Expectations**

- Owner/Operator
- Shareholders/Board
- Insurance Company
- Legal
- Administrators/Service Lines
- Care Providers
- Information Technology
- Forensics
- 3rd Party IT
- Supplemental IT
- Etc...

51 Days to Contain
Implement Appropriate Technical Safeguards

- Hacker are constantly upgrading their tools and techniques

- Legacy vs. Next Gen
  - Antivirus vs Endpoint Detection and Response
  - Firewalls vs Next Gen
  - Email AV vs Secure Email Gateways

- On Network and Off Network

- Mobile Device Exposure

- Air Gap Backup and Disaster Recovery
Test and Inspect

3rd Party Risk Management

External View (Partner and Hacker)
Internal Monitoring and Reaction

Internal (Logging and SIEM)

- Automation of Daily Activities
- System Logs Storage
- Incident Response
- Forensics
- eDiscovery

Build vs. Buy
Privacy & Compliance - Check all the Boxes

- HIPAA
- HiTech
- General Data Protection Rule (GDPR)
- California Consumer Privacy Act
- Payment Card Industry (PCI)
Internet of Things (IoT/MIoT)

- Mobile Devices
- Smart Homes
  - Alexa
  - TV’s
  - Security Camera’s
- Wearables
- Medical Devices
- Biometrics
- Chatbots
Grades from the Field

• **F’s**
  • Haven’t completed a Risk Assessment
  • Don’t have Business Associate Agreement in place
  • Believe Antivirus, Firewall, and Laptop Encryption are good enough

• **C’s**
  • RA and BA are in place and reviewed regularly
  • Investing in additional security technologies to plug holes

• **A’s**
  • Recognize their limitations and monitor their environment
  • Addressing next generation threats
Resources

US Food and Drug Administration

Other Collaborations on Cybersecurity in Medical Devices

**MITRE Corporation:** In October 2018, the FDA supported the development of the MITRE Corporation’s Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook. The playbook describes the types of readiness activities that will enable health delivery organizations (HDOs) to be better prepared for a cybersecurity incident involving their medical devices and gives product developers more opportunity to address the potential for large scale, multi-patient impacts that may raise patient safety concerns.

**Cybersecurity in the News**

- FDA In Brief: FDA proposes updated cybersecurity recommendations to help ensure device manufacturers are adequately addressing evolving cybersecurity threats (October 17, 2018)
- FDA News Release: FDA and DHS increase coordination of responses to medical device cybersecurity threats under new partnership; a part of the two agencies’ broader effort to protect patient safety (October 16, 2018)
- FDA In Brief: FDA warns patients, providers about cybersecurity concerns with certain Medtronic implantable cardiac devices (October 11, 2018)
- FDA Statement: FDA’s efforts to strengthen the agency’s medical device cybersecurity program as part of its mission to protect patients (October 1, 2018)
- FDA News Release: FDA outlines cybersecurity recommendations for medical device manufacturers (January 15, 2016)

https://www.phe.gov/Preparedness/planning/405d/Pages/default.aspx

https://www.fda.gov/medical-devices/digital-health/cybersecurity
Resources

• https://www.nist.gov/cyberframework

• https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity

• https://www.fbi.gov/investigate/cyber

• https://www.dhs.gov/topic/cybersecurity

Discussion

Dennis Ast, CPCU, CCIC
Cyber Insurance Specialist
Dast@OneGroup.com
716-572-2410

Dennis O’Connell
Director
doconnell@Customonline.com
631-513-8847