The Top 5 Cybersecurity Threats to the Healthcare Industry –

How to Identify, Mitigate and Manage Them

June 20, 2019

Presented by:

Michael Shoffner
Senior Manager, Chief Compliance and Security Officer
Michael Shoffner
Chief Compliance & Security Officer

Mike has presented numerous times to audiences at OHCA and has assisted many healthcare clients with cybersecurity prevention in their systems.

His specializations include cybersecurity audits, HIPAA compliance, policy and procedure development, facility operational overviews, IT system interfaces, software release testing, IT risk assessments, corporate compliance and data mining.
Today's Topics

- Current trends in Cybersecurity
- The top 5 Cybersecurity threats to data
- Practical strategies & safeguards for protecting data
- Cybersecurity risk assessments
- HIPAA requirements for protecting privacy
- Data breaches/security incidents
Most Frequently Targeted Industries

- Energy
- Education
- Healthcare
- Government
- Media
- Manufacturing
- Retail
- Professional Services
- Transportation
- Finance and Insurance

© HW&Co. 2019 -- All Rights Reserved
The 2018 Ponemon Cost of a Data Breach study shows the Healthcare Industry has the highest cost per record breached at $408.

This cost is nearly twice the amount of the next-highest industry (Financial Services) and significantly above the average cost of $148.
Types of Actors Involved in Breaches

- External
- Internal
- Partner
- Multiple

Breaches by Year:
- 2010: 0%
- 2011: 20%
- 2012: 40%
- 2013: 60%
- 2014: 40%
- 2015: 20%
- 2016: 0%
- 2017: 0%
Motivation for Breaches

- Financial
- Espionage
- Fun
- Other
- Grudge

Breaches

© HW&Co. 2019 -- All Rights Reserved

Conversations That Change Everything™
Breach Timelines

Compromise, n=171

Discovery, n=562

© HW&Co. 2019 -- All Rights Reserved

Conversations That Change Everything SM
Time to Discovery of a Breach

MEDIAN DWELL TIME

416 DAYS IN 2011

78 DAYS IN 2018

Percent of investigations in 2018:

- 15% (0-7 days)
- 7% (8-14 days)
- 9% (15-30 days)
- 7% (31-45 days)
- 7% (46-60 days)
- 7% (61-75 days)
- 4% (76-90 days)
- 2% (91-150 days)
- 10% (151-200 days)
- 6% (201-365 days)
Internet of Things (IOT) Attacks

**Top Devices**
- Router: 75.2%
- Connected Camera: 15.2%
- Multi Media Device: 5.4%

**Top Passwords Used**
- 123456: 24.6%
- [Blank]: 17.0%

Average Attacks Per Month: 5,233
Mobile Device Issues

- One in 36 had high risk Apps installed or was rooted or jailbroken
- Easily lost/stolen
- Lack of privacy
- Updates depend on model and manufacturer
- Management Nightmare
Breaches by Location of PHI

2018 Healthcare Data Breaches by PHI Location

- Electronic Medical Record: 27
- Desktop Computer: 34
- Network Server: 74
- Email: 122
- Paper/Films: 81
- Other Portable Electronic Device: 35
- Laptop: 27
- Other Portable Electronic Device: 21
2019 Healthcare Data Breaches

Healthcare Data Breaches by Month

<table>
<thead>
<tr>
<th>Month</th>
<th>Breaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sep - 18</td>
<td>25</td>
</tr>
<tr>
<td>Oct - 18</td>
<td>31</td>
</tr>
<tr>
<td>Nov - 18</td>
<td>34</td>
</tr>
<tr>
<td>Dec - 18</td>
<td>23</td>
</tr>
<tr>
<td>Jan - 19</td>
<td>33</td>
</tr>
<tr>
<td>Feb - 19</td>
<td>32</td>
</tr>
</tbody>
</table>
Cause of Healthcare Breaches

<table>
<thead>
<tr>
<th>Cause</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft</td>
<td>4</td>
</tr>
<tr>
<td>Unauthorized Access/Disclosure</td>
<td>4</td>
</tr>
<tr>
<td>Hacking/It Incident</td>
<td>24</td>
</tr>
</tbody>
</table>
Top 5 Threats to Healthcare Data

1] Email attachments and links
2] Mobile/remote email/data access
3] User access permissions
4] Remote Access / Non User Access
5] Theft and loss
4% of people will click on a phishing email
78% of people will NOT click at all
Once someone has clicked on one, 15% will do it again
Only 17% of phishing emails are ever reported
The first click in a phishing campaign is within 16 minutes
If it is going to happen at all, the first click is usually done within an hour
The first report is around 30 minutes, IF it is reported
Email attachments and links, continued

Top Malicious Attachments
- .doc, .dot: 37.0%
- .exe: 19.5%
- .rtf: 14.0%

1 in 3,207 emails was phishing in 2018

Top Attachment Categories
- Scripts / Macros: 47.5%
- Executables: 24.7%
Email attachments and links, continued

48% of all malicious email attachments are office files
Mobile Device Management

- Control Access to Information
- Enforce Policies
  - “Allowed” Applications
  - Encryption
- Allow Security
  - Password Requirements
  - Lock Screen / Time Out
- Remote Wipe of Information
- Sandbox for Corporate Data
Credentials - Passwords

- Each users are unique
- Expire on a set schedule
- Complexity is forced
  - Long phrases are encouraged
- Biometric Logins
- User access rights are defined by Job Title/Function
- Revoked upon Termination or Job Change
Great Example of what NOT to do!
## Credentials – Passwords / User Access

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td></td>
</tr>
<tr>
<td>Position</td>
<td></td>
</tr>
<tr>
<td>Password Expires</td>
<td></td>
</tr>
<tr>
<td>Default Admin Tab</td>
<td>Resident Profile</td>
</tr>
<tr>
<td>Default Care Tab</td>
<td>Resident Profile</td>
</tr>
<tr>
<td>Auto Page Setup</td>
<td></td>
</tr>
<tr>
<td>Enterprise User</td>
<td>(Has access to all facilities)</td>
</tr>
<tr>
<td>Max Failed Logins</td>
<td>Use System Default (in 5 min. period)</td>
</tr>
<tr>
<td>Link to Staff</td>
<td><em>None Linked</em></td>
</tr>
<tr>
<td>Valid Until</td>
<td></td>
</tr>
<tr>
<td>Medical Professional</td>
<td></td>
</tr>
<tr>
<td>External Facility</td>
<td></td>
</tr>
<tr>
<td>Log into Management</td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td></td>
</tr>
</tbody>
</table>

**Alternate Password/PIN Expires:**

- **Remote User:** ✔
- **Disable User Login:**  

**Log into IRM:**  

© HW&Co. 2019 – All Rights Reserved

Conversations That Change Everything™
“You might have a very good password on your bank or investment account, but if your Gmail account doesn’t have a good password on it, and they can break into that, and that’s your password recovery Email, they’ll own you” -- Lance Cottrell

Security is only as good as the weakest link
Education

- Formal yearly security training (HIPAA)
- Quarterly updates as needed
- Monthly reminders
- Daily tips and tricks
- Don’t forget to document all training
Train, re-Train, and Train again, repeatedly….

- Employees should **NEVER**, ever give up their Network Credentials
- Their only normal use is to logon to Corporate Computers
- Even most IT departments do NOT need them
Phishing is a form of **social engineering** that attempts to steal sensitive information.

They most frequently accomplish phishing attacks via email.

The email usually pretends to be from someone trustworthy, like your bank, UPS/FedEx, a credit card company or an airline, or some other site for which you may have login credentials.

The email includes a link to an “official” website that is actually a fake site operated by the attacker.
Education, continued

- **Requests personal information**
  - Phishing emails will commonly ask for a target’s name, phone number, address, account number, social security number, etc.

- **Bad or forged links**
  - Links in phishing emails may look legitimate but upon closer inspection, the target can usually find misspellings or a different suffix than expected, such as .biz instead of .com).

- **Sense of Urgency**
  - Phishers try to create a sense of urgency in their targets, like threatening to close a target’s account or delete their information if they do not respond in a timely manner.
Never open attachments or links in unsolicited emails.

In general, be suspicious of all emails containing links. If you get an email with a link for you to click, do not click it. Navigate independently to the destination site (for example, by typing www.mybigbank.com into a new browser window) and find the referenced location without using the conveniently included link.

Do not respond to suspicious emails in any manner.

Do not access emails on the same computers used to initiate or approve payments.

Make sure management is aware when you receive a suspicious email.
Checking the email address will sometimes show nothing as the email address has been spoofed.

Your first clue could be that the email has a generic salutation. If an email actually came from your own security department, it would probably be addressed to “Martin”, or “Mr. Reyes”, and not to the job role.

The only real clue sometimes in an email is the hyperlink. In most cases hovering over the hyperlink field will show the embedded link without actually opening it. If the hyperlink points to a site that is completely unrelated to the organization, something similar to this: http://jkdev.nodonenet.com/forwarding.htm it’s a bad thing!
Phishing emails are often sent from addresses that look official.

Clicking on this link would take you to a fraudulent website with a form to enter your personal information.

Notice that the URL does not direct you to an official IRS website.
Education, continued

Conversations That Change Everything™

© HW&Co. 2019 — All Rights Reserved
Wow! Looks official, right? It says IRS, it has the logo... etc.

If it sounds too good to be true, then it probably is too good to be true.

Get Started
Hover the mouse over the link, but DO NOT click the link!

Now observe the actual link you would be taken to!
Preventions

ENCRYPTION

- Best get out of jail free card around, but....
- The Encryption Key must be controlled and complex
Email filters can help reduce the volume of emails in any given inbox.

While they may physically be a first line of defense, the human interaction is the last hope of success.

A positive permission system will only allow accepted emails thru.

A filtering system can look at content, attachments, and hyper links.
Preventions, continued

- 2-factor is the BEST protection against a hacker gaining access by either guessing credentials or tricking a user into giving them up.

- Something you know + Something you have
Preventions, continued

SOC 2 REPORT

FOR THE

GOFILEROOM HOSTING SERVICES

A TYPE 2 INDEPENDENT SERVICE AUDITOR’S REPORT ON CONTROLS RELEVANT TO SECURITY AND AVAILABILITY
HIPAA/Hitech Security Rule Framework

**Risk Analysis**

**Administrative Safeguards**
- Authorization and supervision of workforce

**Physical safeguards**
- Facility access
- Removal of electronic media

**Technical safeguards**
- Access controls
- Audit controls
A breach occurs where there is an acquisition, access, use, or disclosure of *unsecured* PHI that:

- Violates the Privacy Rule
- Compromises the security or privacy of the PHI

**Presumption of breach**

**Exceptions**

- Unintentional access by workforce member or agent
- Inadvertent disclosure amongst authorized persons
- Inability to retain information
- Low probability of compromise based on risk assessment
Google Calendar is a “HIPAA compliant” calendar service, as it is included in Google’s BAA. However, unless a signed BAA is obtained by a covered entity PRIOR to using the service in connection with any ePHI, it constitutes a HIPAA violation.
iCloud terms and conditions...

“If you are a covered entity, business associate or representative of a covered entity or business associate (as those terms are defined at 45 C.F.R § 160.103), You agree that you will not use any component, function or other facility of iCloud to create, receive, maintain or transmit any “protected health information” (as such term is defined at 45 C.F.R § 160.103) or use iCloud in any manner that would make Apple (or any Apple Subsidiary) Your or any third party’s business associate.”
Risk Assessment

- **Measurable Results**
  - Quantified
  - Repeatable
  - Weighted output

- **Rating Scale**
  - Severity
  - Likelihood
  - Impact on business
  - Impact on regulations

- **Simple Answers**
  - Yes
  - No
  - N/A
Risk Assessment

Risk Severity Matrix

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Almost Certain 5</th>
<th>Likely 4</th>
<th>Possible 3</th>
<th>Unlikely 2</th>
<th>Rare 1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Moderate</td>
<td>High</td>
<td>Extreme</td>
<td>Extreme</td>
<td>Extreme</td>
</tr>
<tr>
<td></td>
<td>Moderate</td>
<td>Moderate</td>
<td>High</td>
<td>Extreme</td>
<td>Extreme</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
<td>High</td>
<td>Extreme</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
HealthIT.gov has updated their on-line Risk Assessment

It can be downloaded from the following link:

https://www.healthit.gov/sites/default/files/SRA-Tool-3.0.1.msi

Disclaimer

The Security Risk Assessment Tool at HealthIT.gov is provided for informational purposes only. Use of this tool is neither required by nor guarantees compliance with federal, state or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and organizations. The Security Risk Assessment Tool is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks. For more information about the HIPAA Privacy and Security Rules, please visit the HHS Office for Civil Rights Health Information Privacy website.

NOTE: The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management. This tool is not intended to serve as legal advice or as recommendations based on a provider or professional’s specific circumstances. We encourage providers, and professionals to seek expert advice when evaluating the use of this tool.
## NIST Cybersecurity Framework

### Core

*A Catalog of Cybersecurity Outcomes*

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
</tr>
</thead>
</table>
| **Identify** | Asset Management  
| | Business Environment  
| | Governance  
| | Risk Assessment  
| | Risk Management Strategy  
| | Supply Chain Risk Management<sup>1,1</sup> |
| **Protect** | Identity Management, Authentication and Access Control<sup>1,1</sup>  
| | Awareness and Training  
| | Data Security  
| | Information Protection Processes & Procedures  
| | Maintenance  
| | Protective Technology  
| | Anomalies and Events  
| | Security Continuous Monitoring  
| | Detection Processes |
| **Detect** | Response Planning  
| | Communications  
| | Analysis  
| | Mitigation  
| | Improvements  
| | Recovery Planning  
| | Improvements  
| | Communications |
| **Respond** |  
| **Recover** |  

© HW&Co. 2019 – All Rights Reserved
# NIST Cybersecurity Framework

## Core – Example 1.1
### Cybersecurity Framework Component

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
| PROTECT (PR)     | Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. | PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions | CIS CSC, 16  
                  |                                                                          |                                                             | COBIT 5  
                  |                                                                          |                                                             | DSS05.04, DSS05.05, DSS05.07, DSS06.03 |
|                  |                                                                          |                                                             | ISA 62443-2-1:2009  
                  |                                                                          |                                                             | 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 |
|                  |                                                                          |                                                             | ISA 62443-3-3:2013  
                  |                                                                          |                                                             | SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 |
|                  |                                                                          |                                                             | ISO/IEC 27001:2013  
                  |                                                                          |                                                             | A.7.1.1, A.9.2.1 |
|                  |                                                                          |                                                             | NIST SP 800-53 Rev. 4  
                  |                                                                          |                                                             | AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3 |
|                  |                                                                          |                                                             | PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks) | CIS CSC, 1, 12, 15, 16  
                  |                                                                          |                                                             | COBIT 5  
                  |                                                                          |                                                             | DSS05.04, DSS05.10, DSS06.10 |
|                  |                                                                          |                                                             | ISA 62443-2-1:2009  
                  |                                                                          |                                                             | 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 |
|                  |                                                                          |                                                             | ISA 62443-3-3:2013  
                  |                                                                          |                                                             | SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 |
|                  |                                                                          |                                                             | ISO/IEC 27001:2013  
                  |                                                                          |                                                             | A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 |
|                  |                                                                          |                                                             | NIST SP 800-53 Rev. 4  
                  |                                                                          |                                                             | AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 |
Cybersecurity programs that reasonably conform to any of these industry standards qualify:

- Framework for Improving Critical Infrastructure Cyber Security developed by NIST and certain other NIST publications
- The Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework
- The Center for Internet Security Critical Security Controls for Effective Cyber Defense
- Payment Card Industry (PCI) Data Security Standard
For covered entities regulated by the state or federal government, cybersecurity programs that conform to any of these laws qualify:

- **Security Requirements of HIPAA**
- Title V of the Gramm-Leach-Bliley Act of 1999
- **The Health Information Technology for Economic and Clinical Health Act**
Security Incidents

- Need a written incident plan
- Identify key people
- Identify business ‘hot points’
- Identify industry ‘issues’
- Check list approach (yes/no)
Indicia of potential incidents

- Unusual computer system activity
- Unusual employee activity
- Loss of equipment
- Policy violation
Incident Discovery, continued

- Inspect computer logs
- Validate user activity
- Validate IP addresses
- Log failed login attempts
- 2nd Factor
Determine was it a Breach or Not?

Potential Incident of Data Breach Reported

- OH Rev. Code, lit.XIII. ch. 1349, Section 19
  - YES
    - Does it involve a breach of the security of the system that compromises the security, confidentiality or integrity of an individual's private information?
      - YES
        - Does it involve unsecured or unencrypted PHI?
          - YES
            - Reportable Data Breach has occurred
          - NO
        - NO
      - NO
  - NO

- HITECH Act
  - YES
    - Does the incident violate the HIPAA Privacy rule?
      - YES
        - Does it involve unsecured or unencrypted PHI?
          - YES
            - Reportable Data Breach has occurred
          - NO
        - NO
      - NO
  - NO

Not a Reportable Breach
STOP HERE

Does the incident qualify as an exemption?
1) Good faith, unintentional acquisition, access, or use of PHI by the EHR's USERS.
2) Inadvertent disclosure to another authorized person within the entity.
3) Recipient could not reasonably have retained the data.
4) Data is limited to limited data set that does not include dates of birth or zip codes.
5) Satisfactory assurances were obtained that access data will not be used by unauthorized individual.

Does this data breach "pose a significant risk of financial, reputational, or other harm to the individual affected?"
Breach Response

- Regulatory requirements
- Internal requirements
- Leverage internal controls
- Leverage risk assessments
  - Plan ahead, don’t wait until the worst has happened
  - Prepare canned responses
  - Contact Insurance Carrier
Breach Response, continued

- State Agencies / Attorney General
- Federal Agencies
- Consumer Reporting Agencies
- Company Management
- Employees
- Clients
- Media
- Law Enforcement
- Owners of the Breached Information
Nothing is Static, Continual Improvement
Q & A
Let’s Talk...

Michael Shoffner
Senior Manager, Chief Compliance and Security Officer
Email: shoffner@hwco.com
Phone: 877.FOR.HWCO