CYBERSECURITY AND SAFEGUARDING HEALTHCARE RECORDS

ANDREA BAKER
Risk Advisory Services, BDO
IT Manager
abaker@bdo.com
Office: 817-782-2145
Mobile: 817-223-9195
Topics

This discussion contains the following topics:

- Topic 1: Today’s Threat Landscape
- Topic 2: IT Security Maturity Assessment
- Topic 3: Cybersecurity and Its Impacts on Healthcare

Question

The majority of breaches are associated with what kind of threat actors?

A. Internal
B. External
Today's Threat Landscape
Data Breach Threat Actors, Motives, and Methods

<table>
<thead>
<tr>
<th></th>
<th>2019</th>
<th>All Industries</th>
<th>Healthcare</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Actors</td>
<td>External</td>
<td>Internal</td>
<td></td>
</tr>
<tr>
<td>Motives</td>
<td>Financial</td>
<td>Financial</td>
<td></td>
</tr>
<tr>
<td>Compromised Data</td>
<td>Internal</td>
<td>Medical</td>
<td></td>
</tr>
<tr>
<td>Top Threat Actions in Breaches</td>
<td>Hacking (Stolen Creds) Social (Phishing) Malware (Backdoor)</td>
<td>Error (Misdistribution) Misuse (Privilege Abuse) Hacking / Social</td>
<td></td>
</tr>
<tr>
<td>Top Patterns in Breaches</td>
<td>Web Applications Misc. Errors</td>
<td>Misc. Errors (Misdistribution) Privilege Misuse</td>
<td></td>
</tr>
<tr>
<td>Compromised Data</td>
<td>Internal</td>
<td>Medical</td>
<td></td>
</tr>
<tr>
<td>Click rate in phishing tests</td>
<td>(High) Education: 4.93% (Low) Retail: 1.32%</td>
<td>2.13%</td>
<td></td>
</tr>
</tbody>
</table>

2,013 data breaches
304 (15%) Healthcare
41,686 security incidents
466 (1%) Healthcare

Question
Which industry has the highest costs associated with data breaches?
A. Health
B. Financial
Today’s Threat Landscape
Data Breach Costs

Cost of a Data Breach Report

507 companies
3,211 interviews

<table>
<thead>
<tr>
<th></th>
<th>2019 Global Average (All Industries)</th>
<th>Healthcare</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Breach Costs</td>
<td>$3.92M (U.S. = $8.19M)</td>
<td>$6.45M</td>
</tr>
<tr>
<td>Ave Cost / Record</td>
<td>$150</td>
<td>$429</td>
</tr>
<tr>
<td>Abnormal Customer Turnover</td>
<td>3.9%</td>
<td>7%</td>
</tr>
<tr>
<td>Mean Time to Identify (MTTI)</td>
<td>206 days</td>
<td>236 days</td>
</tr>
<tr>
<td>Mean Time to Contain (MTTC)</td>
<td>73 days</td>
<td>93 days</td>
</tr>
</tbody>
</table>

Question

Which is currently a more common cause of healthcare data breaches over 500 records?

A. Improper Disposal
B. Unauthorized Disclosure
Today's Threat Landscape
Healthcare Data Breaches per Year

- 2018:
  - Hacking/IT Incidents (158 breaches)
  - Unauthorized Access/Disclosures (143 breaches)
  - Loss/Theft (55 breaches)
  - Improper Disposal (9 breaches)
- Data breaches reported at a rate of more than 1 / day
- Greatest number of records breached in 2015 (~113 M records)
- Fewest records breached in 2012 (~2.8 M records)
- 2018 - record breaking year for HIPAA fines and settlements
  - $28.6 M from covered entities and business associates

Question

Which covered entity had the largest healthcare data breach since 2009?

A. Premera Blue Cross
B. Anthem Inc.
Today's Threat Landscape
Case Studies

Anthem
2015
78.8M individuals
Hacking/IT Incident

SAIC
2011
4.9M individuals
Loss

ERS
2018
1.2M individuals
Unauthorized Access/Disclosure

AvMed
2010
1.7M individuals
Theft

AccuDoc Solutions
2018
2.6M individuals
Hacking/IT Incident

UnityPoint Health
2018
1.4M individuals
Hacking/IT Incident

Today’s Threat Landscape
Office for Civil Rights (OCR) Breach Portal

![Image of OCR Breach Portal]

Cases Currently Under Investigation:
This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

As required by section 465(a) of the HIPAA Privacy Rule, the Secretary must post a list of breaches of protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary.

<table>
<thead>
<tr>
<th>Covered Entity</th>
<th>Breach Description</th>
<th>Number of Individuals Affected</th>
<th>Date of Breach Report</th>
<th>Type of Breach</th>
<th>Location of Disclosed Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Hospital Association for the Deaf</td>
<td>Hacking/IT Incident</td>
<td>1000</td>
<td>12/31/2019</td>
<td>Hacking/IT Incident</td>
<td>Electronic Medical Record, Email</td>
</tr>
<tr>
<td>North Carolina Department of Correction</td>
<td>Unauthorized Access/Disclosure</td>
<td>5000</td>
<td>01/01/2020</td>
<td>Unauthorized Access/Disclosure</td>
<td>Electronic Medical Record, Paper Medical Records</td>
</tr>
<tr>
<td>HealthCity</td>
<td>Hacking/IT Incident</td>
<td>2500</td>
<td>02/02/2020</td>
<td>Hacking/IT Incident</td>
<td>Electronic Medical Record, Paper Medical Records</td>
</tr>
<tr>
<td>iHealth</td>
<td>Hacking/IT Incident</td>
<td>1500</td>
<td>03/03/2020</td>
<td>Hacking/IT Incident</td>
<td>Electronic Medical Record, Paper Medical Records</td>
</tr>
<tr>
<td>University of Alabama at Birmingham</td>
<td>Hacking/IT Incident</td>
<td>5000</td>
<td>04/04/2020</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
<tr>
<td>Federico J. Wheeler, CRNP</td>
<td>Hacking/IT Incident</td>
<td>1000</td>
<td>05/05/2020</td>
<td>Hacking/IT Incident</td>
<td>Electronic Medical Record, Paper Medical Records</td>
</tr>
</tbody>
</table>
Overview
An IT security maturity assessment is used to give a company a high level idea of their current IT state by assessing the risk and maturity levels of their IT environment. This is done by determining any gaps in program design, policies, standards, and procedures.

Framework
Our approach and methodology leverages the National Institute of Standards & Technology (NIST) Cybersecurity Framework to evaluate the cybersecurity maturity and level of risk, in comparison to other organizations of similar size and industry.

Why NIST?
The NIST Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber attacks.
IT Security Maturity Assessment
NIST Recommended Cybersecurity Components

NIST Cybersecurity Framework

**Identify**
- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

**Protect**
- Access Control
- Awareness and Training
- Data Security
- Info Protection Processes and Procedures
- Maintenance
- Protective Technology

**Detect**
- Anomalies and Events
- Identity Continuous Monitoring
- Detection Processes
- Maintenance
- Protective Technology

**Respond**
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

**Recover**
- Recovery Planning
- Improvements
- Communications

---

IT Security Maturity Assessment
Risk Scorecard

<table>
<thead>
<tr>
<th>Category</th>
<th>Score</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Security</td>
<td>3.00</td>
<td>3.00</td>
</tr>
<tr>
<td>Configuration Management Control</td>
<td>3.00</td>
<td>3.00</td>
</tr>
<tr>
<td>Contingency Planning</td>
<td>3.00</td>
<td>3.00</td>
</tr>
<tr>
<td>Data Protection</td>
<td>3.00</td>
<td>3.00</td>
</tr>
<tr>
<td>Incidence</td>
<td>3.00</td>
<td>3.00</td>
</tr>
<tr>
<td>Identity Management &amp; Access Control</td>
<td>3.00</td>
<td>3.00</td>
</tr>
<tr>
<td>Incident Response</td>
<td>3.00</td>
<td>3.00</td>
</tr>
<tr>
<td>Identity Management &amp; Access Control</td>
<td>3.00</td>
<td>3.00</td>
</tr>
<tr>
<td>Governance</td>
<td>3.00</td>
<td>3.00</td>
</tr>
</tbody>
</table>
IT Security Maturity Assessment
Greatest Risks and Common Findings

Cybersecurity Governance - The policies, standards, and processes to manage and monitor standards and procedures around cybersecurity haven’t been formally documented

Incident Response - Lack of procedures and policies in place to detect, respond, and contain the negative impact of an incident threatening the security of the organization’s business processes

Data Protection - Lack of data security protection consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information

Threat Intelligence - Limited risk processes and security technologies in place to ensure that the information systems cannot be exploited using known vulnerabilities

Cybersecurity and Impacts on Healthcare
Digital Transformation

- Increase use of IoT devices in the healthcare industry
- Attack surface is growing
- Health information sharing methods (mobile)
- Health information storing methods (cloud-based)
Cybersecurity and Impacts on Healthcare

Changes in the way we access, transmit, and store health information

- Websites
- Mobile Access
- Text (SMS)
- Virtual Patient Visits
- Social Media
- Cloud Computing

Cybersecurity and Impacts on Healthcare

Legislation

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Applies to:
  - Covered Entities - transmit protected health information for transactions for which the Department of HHS has adopted standards
  - Business Associates - provide services to a HIPAA-covered entity which requires them to have access to, store, use, or transmit protected health information
  - Rules include:
    - Security Rule (Safeguards)
    - Privacy Rule
    - Breach Notification Rule
    - Omnibus Rule
    - Enforcement Rule

- The Health Information Technology for Economic and Clinical Health (HITECH) Act - 2009
- The Medicare Access & CHIP Reauthorization Act of 2015 (MARCA)
Cybersecurity and Impacts on Healthcare

HIPAA Security Rule

- HIPAA Security Rule
  - Standards that must be applied to safeguard ePHI when it is at rest and in transit
  - Includes “required” and “addressable” safeguards on the HIPAA compliance checklist
  - Three parts:
    - Technology Safeguards
    - Physical Safeguards
    - Administrative Safeguards

HIPAA Privacy Rule

- HIPAA Privacy Rule
  - Patients have rights to obtain, examine, and request corrections to their health information
  - Covered entities must respond to patient access requests within 30 days
  - Notices of Privacy Practices (NPPs) must be issued to let patients and plan members know of circumstances when their data will be used or shared
  - Employees must receive training on what information may/may not be shared
  - The integrity of ePHI and individual personal identifiers must be maintained
  - Obtain written permission from patients before using health information for marketing, fundraising or research
Cybersecurity and Impacts on Healthcare

HIPAA Breach Notification Rule

- HIPAA Breach Notification Rule
  - Must notify patients when there is a breach of their ePHI
  - Breach notifications must be made no later than 60 days following discovery
  - Must promptly notify the Department HHS and issue notice to the media if breach affects >500 patients
  - Must report breaches <500 patients via the OCR web portal
  - Defines what must be included in breach notifications

HIPAA Omnibus Rule

- HIPAA Omnibus Rule
  - Amended definitions, clarified procedures and policies, and expanded the HIPAA compliance checklist to cover Business Associates and their subcontractors
Cybersecurity and Impacts on Healthcare

HIPAA Enforcement Rule

- HIPAA Enforcement Rule
  - Governs the ePHI data breach investigations
  - Governs the penalties for covered entities
  - Governs hearing procedures

[True or False] State attorneys general can issue HIPAA violation fines.

A. True
B. False
Cybersecurity and Impacts on Healthcare Legislation

- HIPAA fines issues by:
  - Dept of HHS’ Office for Civil Rights (OCR)
  - State Attorneys General

- Violations are usually discovered by:
  - Data breach investigations
  - Compliant investigations
  - Compliance audits

Question

[True or False] Heart rate and blood pressure information collected from a device manufacturer and/or application that has not been contracted by a HIPAA-covered entity is still considered PHI.

A. True
B. False
Cybersecurity and Impacts on Healthcare

What is considered Protected Healthcare Information (PHI)

- Any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA-covered entity
  - Names
  - Dates, except year
  - Telephone numbers
  - Geographic data
  - Fax numbers
  - SSN
  - Email addresses
  - Medical record numbers
  - Account numbers
  - Healthcare plan beneficiary numbers
  - Certificate/license numbers
  - Vehicle identifiers (including license plates)
  - Driver’s license numbers
  - Web URLs
  - Device identifiers/serial numbers
  - IP addresses
  - Full face photos
  - Biometric identifiers
  - Unique identifiers (numbers/codes)

Most Common HIPAA Violations

- Failure to perform risk analysis to identify risks to CIA of PHI
- Failure to enter into a HIPAA-compliant business associate agreement
- Impermisssible disclosures of PHI
- Not meeting the breach notification deadline
- Failure to safeguard PHI
- Snooping on health records
- Lack of risk management processes
- Failure to use encryption on portable devices
- Improper disposal of PHI
- Denying or exceeding timeframe to provide access to health records
Cybersecurity and Impacts on Healthcare
Common Violations by Healthcare Employees

- Emailing ePHI to personal email
- Unattended paperwork / portable devices
- Releasing PHI to unauthorized individual
- Releasing PHI without authorization
- Releasing PHI to third party after authorization expiration
- Failure to perform risk analysis to identify risks to CIA of PHI
- Impermissible disclosures of PHI
- Downloading PHI to unauthorized devices
- Unauthorized access to PHI
- Failure to enter into a HIPAA-compliant business associate agreement

Cybersecurity and Impacts on Healthcare
Best Practices

- Data encryption
- Phishing awareness
- Audit logs
- Proper network, software, and cloud-based solution configuration
Resources

- https://enterprise.verizon.com/resources/reports/dbir/
- https://www.hipaajournal.com/
- https://www.hhs.gov/hipaa/index.html
- https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- https://www.bdo.com/digital/whitepapers

QUESTIONS?
BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 650 independent alliance firms located nationwide. As an independent Member Firm of BDO International Limited, BDO serves multinational clients through a global network of more than 80,000 people working out of nearly 1,600 offices across over 160 countries and territories.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms.

www.bdo.com