Modeling Factors Associated with Healthcare Data Breaches

Session #155, March 3, 2018
Dr. Alex McLeod, Dr. Diane Dolezel, Texas State University
Conflict of Interest

Alex McLeod, PhD
Diane, Dolezel, EdD, RHIA, CHDA

Has no real or apparent conflicts of interest to report.
Agenda

• Introduce the topic and provide background information
• Discuss current research project
• Look at conceptual frameworks
• Opportunities for modeling data
• Consider big data industry level analysis
• What can individual organizations do?
Learning Objectives

• Recognize opportunities to model exposure, security and organizational factors

• Identify data opportunities to assess vulnerabilities in organizations

• Hypothesize factors associated with the level of exposure, the level of security and the organization to create a testable research question
Introduction

• Preventing healthcare data breaches is hard
• Organizational data breaches have many negative effects
• Breach reporting significantly lags breach detection
Hard to Prevent Data Breaches

• Connected systems increase risk
• Information exchange across multiple platforms
• Multiple connected devices with remote access
• Wireless connections through mobile devices
• Challenge managing Bring Your Own Device (BYOD)
Negative Effects are Substantial

- Disruption of Services
- Loss of revenue
- Costs of breach detection
- Government Fines imposed
- Possible litigation by affected parties
- Consumer’s lose trust in organization
Breach Frequency Increasing

- There were 351 data breaches reported during the first half of 2017
- This amounts to two breaches a day
- Department of Health and Human Services breaches affecting over 500 records for 2009-2017
- Most data breaches from lost or stolen devices, or hacking and IT incidents

Breach Reporting

• Significantly lags behind breach detection
• Federal laws dictate OCR & consumers notified of breaches within 60 days
• Breach detection often occurs many days after breach
• Consumer notifications often delayed
• Cybersecurity breach containment measures inadequate
Example

- Hackers had access to the practice's server
- Cancer center data breach undetected for several months
- Consumers not notified until 5 months after the detection, no reason stated
- Lag time allowed malicious agents to scrutinize 22,000 patients' records for several months
- Social Security numbers, addresses, phone numbers, DOB, and insurance information

## How and Why?

<table>
<thead>
<tr>
<th>ABC Healthcare</th>
<th>MI</th>
<th>Healthcare Provider</th>
<th>16000</th>
<th>10/21/2016</th>
<th>Hacking/IT Incident</th>
<th>Network Server</th>
<th>No</th>
</tr>
</thead>
</table>

- Hacking/IT Incident involving a Network Server
- What security was in place?
- Employee training?
- Email? USB? Insider?
- Wireless access?
- Anti-Malware? Intruder detection?

Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
Greater Understanding Needed

• Examine organizations experiencing data breaches
• Model factors associated with breaches
• Offer insight into health organizations’ risk characteristics

<table>
<thead>
<tr>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Covered Entity Type</th>
<th>Individuals Affected</th>
<th>Breach Submission Date</th>
<th>Type of Breach</th>
<th>Location of Breached Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MO</td>
<td>Healthcare Provider</td>
<td>1000</td>
<td>02/21/2018</td>
<td>Unauthorized Access/Disclosure</td>
<td>Other</td>
</tr>
<tr>
<td></td>
<td>MA</td>
<td>Healthcare Provider</td>
<td>2450</td>
<td>02/05/2018</td>
<td>Hacking/IT Incident</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td></td>
<td>KY</td>
<td>Health Plan</td>
<td>11248</td>
<td>02/05/2018</td>
<td>Unauthorized Access/Disclosure</td>
<td>Paper/Films</td>
</tr>
<tr>
<td></td>
<td>MI</td>
<td>Healthcare Provider</td>
<td>544</td>
<td>02/05/2018</td>
<td>Loss</td>
<td>Other Portable Electronic Device</td>
</tr>
<tr>
<td></td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>6781</td>
<td>02/02/2018</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
</tbody>
</table>
More Data Needed

- What data is organizational available?
- What factors are associated with a breach?
- Where can we get such data?

Organizational Incident Model adapted from Reason (2016)
Compliance Frameworks

• Health Insurance Portability and Accountability Act (HIPAA) Security Rule
• Health Information Technology for Economic and Clinical Health Act (HITECH)
• Joint Commission
• Commission on Enhancing National CyberSecurity
• Department of Health and Human Services (DHHS)
• Department of Homeland Security (DHS)
NIST Framework

- Organizational
- Business Processes
- Technological

Chain of Event Factors

Strategic

Tactical
Organizational Incident Theory

Organizational Incident Model adapted from Reason (2016)
Level of Exposure (Business Processes)

- Internet Connectivity
- Wifi
- HIE participation
- EHR
- CPOE
- Internet of Things

- Patient Portal
- Number of Workstations
- CDSS
- Cloud Storage
- Data Backup
Level of Security (Technological)

- Biometric technologies
- Vulnerability analysis systems
- Barcoding
- Auto Identification
- Intruder detection systems
- Honey pots
- Telecommunication systems
- Risk management systems
- System logging
- Mobile device management systems
- Anti-malware
- Encryption
Organizational Factors

• Security culture
• Employee security training
• Security budget
• IT governance best practices
• Security policies
• Business associate review

• Payroll expense
• Number of beds
• Age of institution
• Operating expense
Research Questions

1. Is there a relationship between the level of exposure and a data breach?
2. Are there factors associated with the level of security and a data breach?
3. Do specific organizational factors appear when there is a data breach?
4. What is the relationships between level of organizational factors, level of exposure and level of security and the likelihood of the occurrence of a data breach?
Data Available

- HIMSS Analytics Legacy Database
  - 6,600 healthcare organizations
- DHHS Data Breach Report
  - 1,804 breach incidents
- Other healthcare databases available
- CMS data
Analysis

• Dependent variable was breach/nobreach
• Independent variables factors extracted from database
• Grouped in constructs
  – level of exposure
  – level of security
  – organizational factors
• Binary logistic regression predict likelihood of data breach
Results – Level of Exposure

• Percent of affiliated physicians using CPOE system
• Percent of personnel using an EMR system
• Presence of a Neonatal Intensive Care Unit
• Number of Intensive Care Beds
• Total number of individuals seen as outpatients
Results – Level of Security

• Barcoding used in hospital laboratories
• Health Information Exchange participation plan

• Marginal
• Barcoding used in the hospital pharmacy
Results – Organizational Factors

• Number of births
• Number of beds
• Number of surgical operations
• Operating expenses
• Year opened
Results – All Factors

• Percent of affiliated physicians using the CPOE system
• Barcoding used in the hospital laboratories
• Number of births
• Number of staffed beds
• Number of surgical operations
• Total operating expense
• Year opened
Limitations

• DHHS reporting requirement of 500 records means that smaller breaches are not reported
• Study was exploratory due to limited research to guide the study
• The DHSS database contained data from 2009-2017
• The HIMSS Analytics Legacy Database contained data from 2015
Discussion

• Contains results from all three types of factors
  – Exposure
  – Security
  – Organizational

• Significant variables indicate
  – Greater technology use
  – Age of organization
  – Complexity of organization
Questions

• Dr. Alex Mcleod, am@txstate.edu

• Dr. Diane Dolezel, dd30@txstate.edu

• Please complete online session evaluation