Mitigating the Number of Impacted Records, Risk Management and Reporting

Martin Ignatovski, Ph.D.

1

AGENDA

01
Introduction
Introduction and definitions

02
Data
Data analysis and data findings

03
Risk Management
Risk management and risk mitigation strategy

04
Summary
Wrapping it all up

2

01

Introduction

3

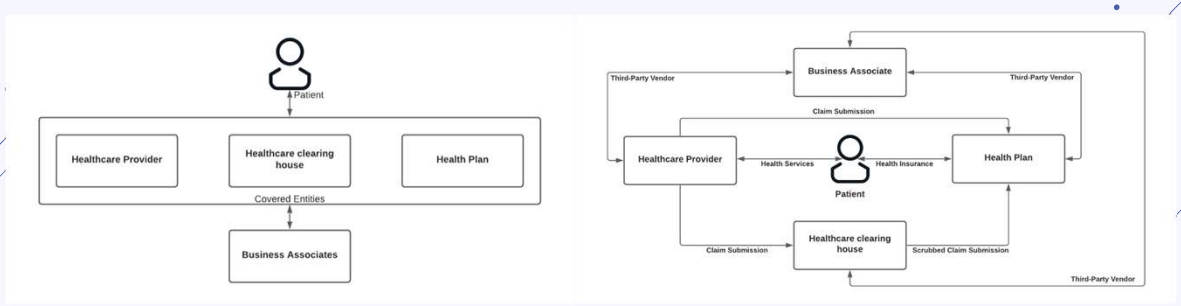
Martin Ignatovski

Dr. Martin Ignatovski serves as the CIO at SimplePractice. He has over 15 years of experience leading and managing technology teams in health technology organizations. Martin is passionate about cybersecurity and contributes to the profession through practice and research.

4

Definitions

HIPAA. Privacy Rule. Security Rule. Breach Notification Rule.
Covered Entity. Business Associate. HHS. Reporting Requirements



5

$7.13 M

average cost of a breach for healthcare entities

$20.8 B

cost of ransomware attacks in US healthcare

18 MILLION

patient medical records exposed, blocked, or stolen

6

329 DAYS

average time to identify and contain a healthcare breach

24%

percentage of breaches in healthcare

700 +

number of clinics, hospitals, and providers affected

7

Why attack healthcare?

Soft target

Large application/technology footprint and internet-facing presence.

We don't do a great job protecting information systems and assets.

Distraction

Recovering from furloughs.

Adjusting to remote workforce.

8

02

Data Analysis and Findings

9

Reporting Requirements

- CEs and BAs must report breaches with over 500 records to HHS and the media.
- HHS portal contains data on breaches since 2009.
- Factors in the data analysis
  - Healthcare entity type: provider, health plan, clearinghouse, and business associate.
  - Data breach type: hacking/IT incident, improper disposal, loss, theft, unauthorized disclosure
  - Data breach location: desktop computer, electronic medical record, email, laptop, network server, portable electronic device, paper/films, other.

10

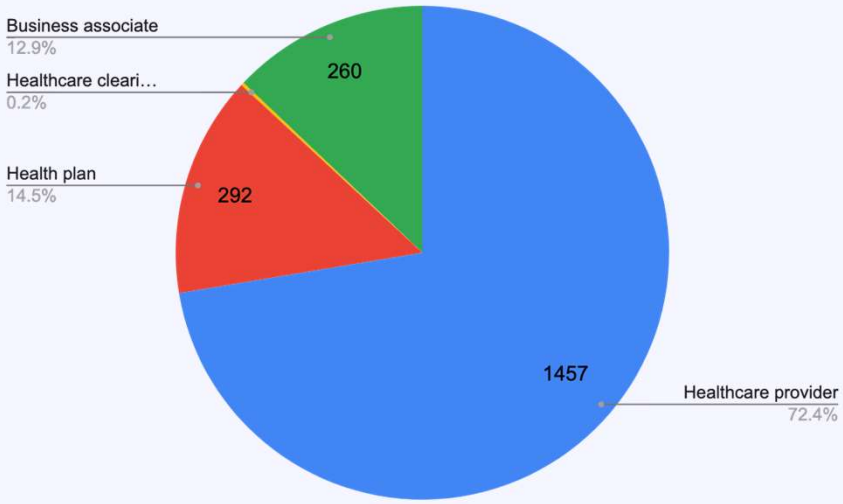
Healthcare entity type, breach type and breach location significantly affect the number of breached medical records.

INITIAL FINDINGS

*Based on data from 2009 and 2020

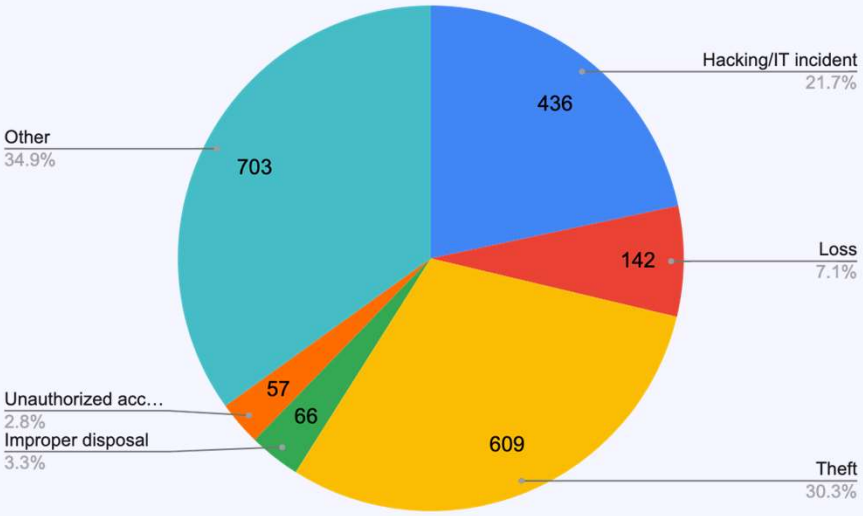
11

Healthcare Entity Type Statistics



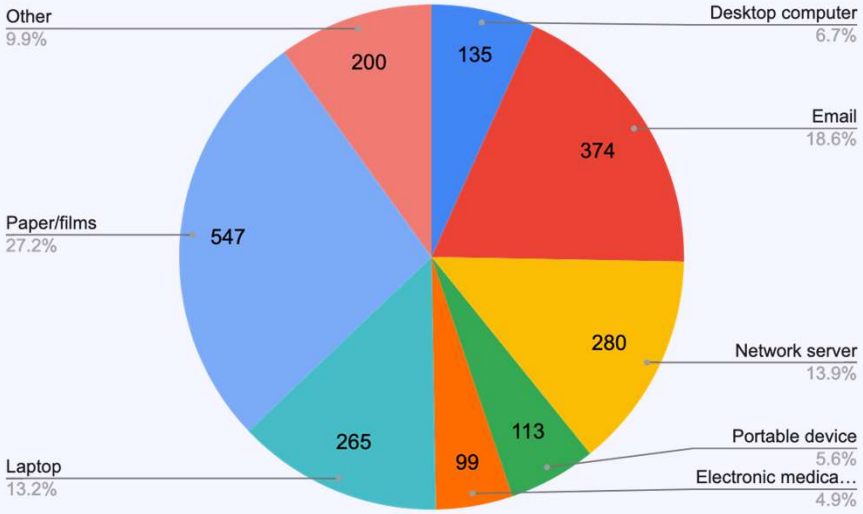
12

Breach Type Statistics



13

Breach Location Statistics



14

Cross-reference

Breach Location: Desktop Computer

- Theft of desktop computer (workstation/laptop) leads to highest number of records breached by healthcare providers
- Health plans gets most records breached in desktop computer by theft and hacking/IT incident
- Hacking/IT incident was the primary reason why business associated breached the most records in desktop computer, followed by unauthorized access and theft

15

Cross-reference

Breach Location: Electronic Medical Record

- Theft and hacking incident were the biggest contributing factor for the highest number of electronic medical records breached by healthcare providers
- Health plans had the most electronic medical records impacted by a hacking/IT incident
- Hacking/IT incident caused the highest number of electronic medical records breached by business associates

16

Cross-reference

Breach Location: Email

- Healthcare providers experienced the highest number of breached records by stolen email credentials/theft and hacking/IT incident
- Health plans experienced the highest number of breached records by stolen email credentials/theft, hacking/IT incident and unauthorized disclosure
- Business associated experienced the highest number of breached records due to hacking/IT incidents, unauthorized disclosure and theft

17

Cross-reference

Breach Location: Laptop

- Healthcare providers experienced the highest number of breached records by having laptops lost by employees. The second highest cause for breached records in laptops was unauthorized access
- Health plans experienced the highest number of breached records by having employee laptops stolen, followed by loss of laptops
- Business associated experienced the highest number of breached records by having laptops stolen from their employees, followed by loss

18

Cross-reference

Breach Location: Network Server

- Hacking/IT incident and theft were the biggest contributing factors to the number of breached records by healthcare providers
- Health plans experienced the highest number of breached records due to theft and unauthorized access/disclosure
- Business associated experienced the highest number of breached records by hacking/IT incident

19

Cross-reference

Breach Location: Portable Electronic Devices

- Improper disposal is the biggest contributing factor to the number of breached records by healthcare providers
- Health plans experienced the highest number of breached records due to unauthorized access/disclosure
- Business associated experienced the highest number of breached records due to loss

20

Cross-reference

Breach Location: Paper/Films

- Improper disposal and hacking/IT incident were the biggest contributing factors to the number of breached records by healthcare providers
- Health plans experienced the highest number of breached records due to improper disposal
- Business associated experienced the highest number of breached records by unauthorized access and theft

21

03

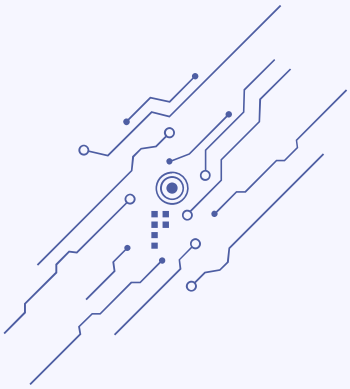
Risk Management and Mitigation

22

Attack Methods & Techniques

Attack trends

- Vulnerabilities, missing patches, and exploits
- Leveraging supply chain breaches to gain a foothold
- Backdoor installations
- Active Directory admin access and GPO
- Password weaknesses and brute force attacks
- Phishing
- High sophistication, long-term planning, disregard for collateral damage

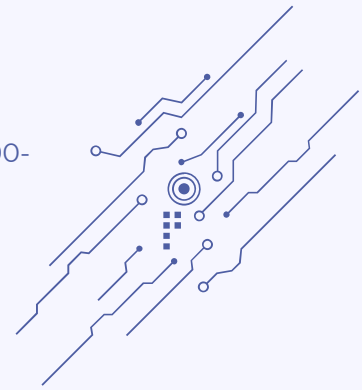


23

Risk Analysis

Comprehensive HIPAA risk analysis is crucial to prepare for the mitigation efforts post-breach occurrence.

- The Security Rule does not prescribe a specific risk analysis methodology
- HHS has issued guidance that provides definitions and reference standards including NIST 800-66 and NIST 800-30



24

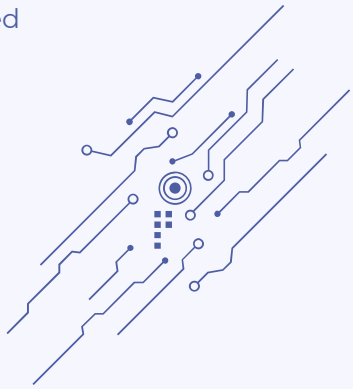
Risk Analysis

HITECH Act Amendment 7898

Introduces safe harbors for HIPAA compliance enforcement by OCR for healthcare entities that adopt certain "recognized security practices"

Examples of recognized security practices:

- HITRUST CSF adoption and certification
- NIST CSF adoption

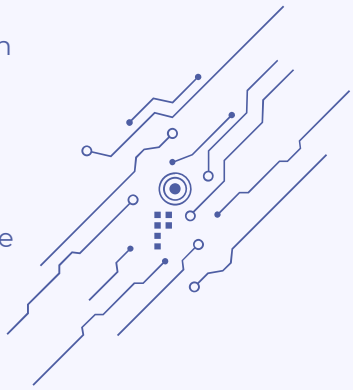


25

Risk Analysis

Minimum considerations for comprehensive risk analysis

PATIENT INFORMATION DISCOVERY · Where is our patient information?
THREATS ACTORS · Who are the bad guys and how likely are they to interact with our environment?
THREAT VECTORS · What are the bad things that can happen and how likely are they to occur?
VULNERABILITIES · How exposed are we & what weaknesses or security holes exist in our environment?
IMPACT ANALYSIS · If we have a bad day, how bad of a day will it be?
RISK DETERMINATION · What are the most pressing areas we need to address?
CORRECTIVE ACTION PLANNING · HOW DO WE FIX WHAT WE FOUND?

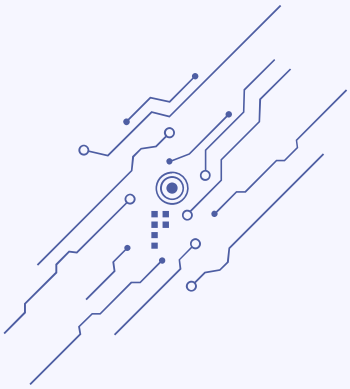


26

Patient Information Discovery

Where is our patient information?

- Identify all locations and functions where patient information is created, received, maintained, or transmitted
- Note: standard sampling methodologies are often used to assess control effectiveness rather than assessing every single asset in the organization
- Assessing only the EHR and top-tier servers is insufficient

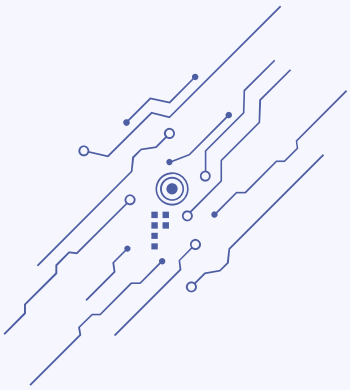


27

Threat Actors

Who are the bad guys and how likely are they to interact with our environment?

- Identify potential threat actors and rank the likelihood that those actors or groups of actors will expose or impact patient information
- Likelihood may vary depending on your organizational type, size, and profile
- Stay up to speed with the latest threat actors

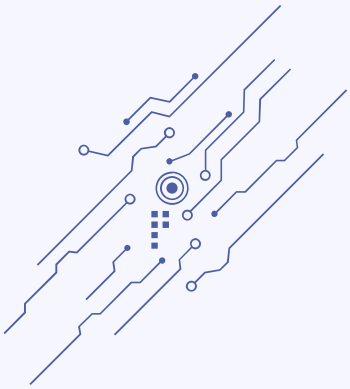


28

Threat Vectors

What are the bad things that can happen, and how likely are they to occur?

- A threat vector is a path or means by which an individual or event can gain access to an organization's information environment to disrupt operations or obtain patient information.



29

Vulnerabilities

How exposed are we, and what weaknesses or security holes exist in our environment?

- NIST defines a vulnerability as "[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy"
- Ongoing identification of security weaknesses
- Deploy vulnerability scanning tools
- Conduct routine ethical hacking and penetration tests
- Conduct routine organizational and application risk assessments

30

Impact Analysis

If we have a bad day, how bad of a day will it be?

- Not all breaches are alike in scope, scale, or impact
- Breach types and thresholds should be assigned to categorize and approximate the potential impact of breach events
- Security incidents and breach events can inflict impacts in the following areas:

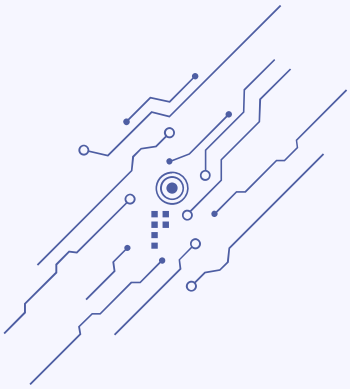

Operational Disruption


Financial Loss


Regulatory Enforcement


Patient Safety


Reputational Damage



31

Risk Determination

What are the most pressing areas we need to address?

- Risk ratings help the entity to prioritize security controls and asset protections
- Risk ratings should consider the factors we have reviewed today including:

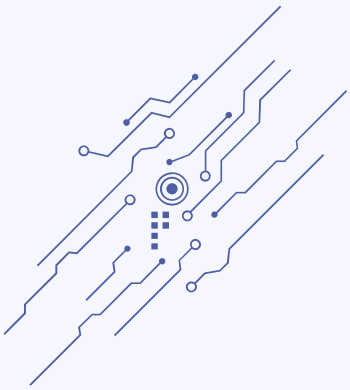

Threat Actors


Threat Vectors


Vulnerabilities


Breach Impacts


Likelihood of Occurrence



32

Corrective Action Planning

How do we fix what we found?

- Identify the greatest risks to the organization
- You can't remediate everything all at once
- Prioritize risks and transition to corrective action planning
- Maintain a risk register and communicate routinely with leadership
- Identify risk owners, timelines, costs, resources, and executive approval for each risk item
- Document risk remediation decisions

33

04

Summary

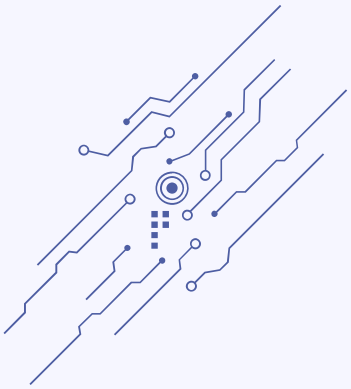
34

Summary

What did we cover today?

- We saw significance on how records are impacted in a healthcare breach
- Use the data, based on your organization, and implement appropriate controls
- Perform comprehensive risk analysis and manage risk

Let's not forget: **Mitigation becomes prevention when the number of impacted records reaches 0!**



35

THANK YOU !

Questions?

Contact:
linkedin.com/in/drmartini

36