Thinking *Inside* the Box:
How to Identify and Tackle Insider Cyber Threats

Michael W. Chase
Abigail T. Mohs

August 12, 2019

Agenda

- Review insider cyber threats in healthcare organizations
- Identify the risks related to cybersecurity incidents
- Practical tips to protect against cybersecurity insider threats

Insider Threat

Ransomware, malware, business e-mail compromise, phishing/whaling, etc. – are all part of a (growing) trend termed the "insider threat"

It's on OCR's Radar & Other Regulators'

"FAILED TO CONDUCT AN ACCURATE AND THOROUGH RISK ANALYSIS OF POTENTIAL RISKS AND VULNERABILITIES TO THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF ALL ITS EPHI"

BH | BAIRDHOLM LLP ATTORNEYS AT LAW

How Big is the Insider Threat?

Threat actors	N	percent
Online scam artist (e.g., phishing, spear phishing)	**56**	**37.6%**
Negligent insider (well-meaning but negligent individuals with trusted access who may facilitate or cause a data breach or other cyber incident)	**31**	**20.8%**
Hacker (e.g., cybercriminal, script kiddie, or other bad actor)	**30**	**20.1%**
Malicious insider (bad actors with trusted access who seek to steal information or damage IT infrastructure)	8	5.4%
Social engineer (e.g., vishing or otherwise) (not via online means)	7	4.7%
Hacktivist (hacking for a politically or socially motivated purpose; not a nation state actor)	6	4.0%
Don't know	6	4.0%
Nation state actor	3	2.0%
Other	2	1.3%

BH | BAIRDHOLM LLP ATTORNEYS AT LAW

(Former FBI) Expert's Perspective

Robert (Bob) Kardell
(402) 636-8313
bkardell@bairdholm.com

BH | BAIRDHOLM LLP ATTORNEYS AT LAW

Who are the Insiders?

- Current Employees
- Former Employees
- Third Party Vendors (remember Target?)
- Outsourced Work
  - Recent Capital One data breach (rented servers)
- Who all has credentials at your organization?

Types of Insider Threats

•Malicious (Bad Actor)
A "Malicious Insider" make a conscious decision to intentionally commit theft or cause harm to an organization

•Negligent
A "Negligent Insider" has awareness of a corporate data security policy, but chooses to ignore it (it's inconvenient)

•Inadvertent (Accidental)
An "Inadvertent Insider" makes a mistake and sends information to someone who should not have received it

Insiders: What are They After?

•Financial Information
- –HR information
- –Customer financial information

•Business Information
- –Marketing/Sales strategies
- –Trade secrets/intellectual property

•Industry-specific information?
- –Patient Information
- –"Big Data"

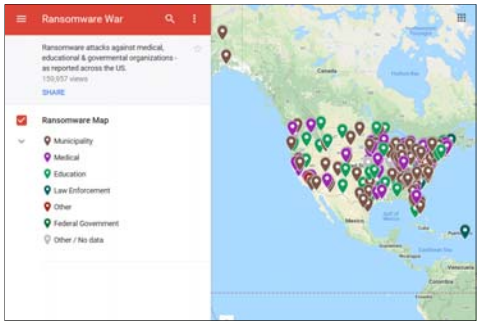
Insiders: The Dangers

- Can go undetected for years
- Hard to distinguish harmful acts with regular business
- Easy to cover tracks
- Difficult to prove guilt

Insiders: Possible Warning Signs

- Unusual data movement
- Unauthorized access attempts
- Suspicious employee behavior
- Stolen credentials
- Policy violations
- Disgruntled employee/Unusually enthusiastic employee
- Uptick in frequency of travel
- Unexplained change in financial circumstance

So…What Happens?



https://www.google.com/maps/d/viewer?mid=1UE6Nko9iRG1tLci_AeqqsxzxGzs&ll=35.935125473972 21%2C-97.34848677802608&z=3

BH | BAIRDHOLM LLP ATTORNEYS AT LAW

Here's How It Begins...

From: <Name of executive / CEO / CFO> <corporate email address>
Reply-To: <Name of executive / CEO / CFO> <non-corporate email address>
To: <Targeted victim in HR / Finance>
Subject: SALARY REVIEW

Hello

Kindly send me the 2015 W-2 (PDF) of all our company staffs for a quick review

Thanks

BH | BAIRDHOLM LLP ATTORNEYS AT LAW

It L  ks Legitimate

From: IRS Online <ahr@lnxt.com>
Reply-To: "noreply@lnxt.com" <noreply@lnxt.com>
Date: Thursday, April 11, 2013 12:15 PM
Subject: Final reminder: Notice of Tax Return. ID: I3HS83326/13

IRS

Department of the Treasury
Internal Revenue Service

04/11/2013
Reference: I3HS83326/13

Claim Your Tax Refund Online

Dear Taxpayer,

We identified an error in the calculation of your tax from the last payment, amounting to $ 319.95.

In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.

Please click "Get Started" below to claim your refund:

Get Started

Link has nothing to do with IRS (or IRS.gov)

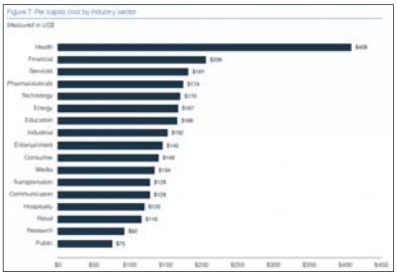
BH | BAIRDHOLM LLP ATTORNEYS AT LAW

Here's How It Ends...

Just Imagine ...

It Could Happen to You!

Cost of a Data Breach



https://healthitsecurity.com/news/healthcare-data-breach-costs-remain-highest-among-industries

Ransomware $$$ Up

- All of 2015: $24M
  - –Average demand: $295
- All of 2016 total: $1B
  - –Average demand: $ 679
- 2017 average demand: $1,077
- 2018 average demand: $522
  - –"High end" demands exceeding $15,000

Ransomware Activity Up

- Healthcare and financial services hit hardest
- Most infections come from emails
- Every 40 seconds, another business is attacked
- 22% of victims had to cease operations after attack
- 1 in 6 experienced 25+ hours of downtown (imagine that!)
- Expected to cost the global economy $6 Trillion per year by 2021
- Recovery costs are outweighing demand

Ransomware Attacks


Patients diverted to other hospitals after ransomware locks down key software

Crypto-extortion increasingly targets bigger victims; most stay silent about it.

by Sean Gallagher - Feb 17, 2016 8:56am CST

Passwords

- "Keys to the castle"
- Email password
- Strong passwords
- Two-factor authentication
- Password manager

Force Thoughtfulness

- Auto-completion on recipient email addresses
- Overcoming employees who believe that the policy doesn't apply to them

"Nebraska Nice"

- Desire to help
- The KEY to social engineering
- Fail to challenge
  - Hold door open
- Assume innocence
- Out of Office messages?

Remember This …

From: <Name of executive / CEO / CFO> <corporate email address>
Reply-To: <Name of executive / CEO / CFO> <non-corporate email address>
To: <Targeted victim in HR / Finance>
Subject: SALARY REVIEW

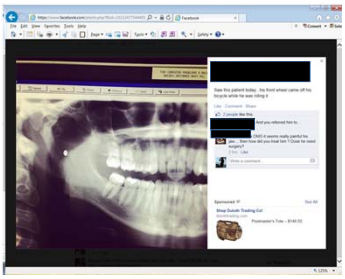
Hello

Kindly send me the 2015 W-2 (PDF) of all our company staffs for a quick review

Thanks

More Insider Threats

Facebook, Snapchat, Twitter

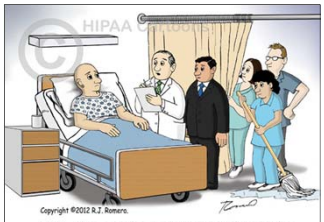


Social Network Landmine

(It's this easy!)

Example (No HIPAA Violation) – but you get the point!

Snooping is *Still* a Problem



"No, they aren't medical students. It's just some of our staff that accessed your Electronic Medical Record and wanted to see that special tattoo."

HIPAA Requirements

- Covered Entities have an obligation to implement administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of protected health information
- Must conduct a "Security Risk Analysis"
- OCR is putting the "pedal to the metal" on enforcement*

* Deven McGraw, Former Deputy Director for Health Information Privacy at HHS, Office for Civil Rights

HIPAA Requirements

- Security Risk Assessment (for HIPAA and Meaningful Use)
  - Conduct/review each reporting period
  - Mitigating risks? Timeline updated?

Security Controls

- Review employee access for the two following principles:

Need to Know: Identifying access based on what data users need to perform job duties

Least Privilege: Granting users access to only that data users need to perform job duties

- And then…MONITOR ACCESS

Other Items to Think About

- Bring Your Own Device ("BYOD")
  - Hospital issued vs. Employee owned
  - Personal use on Hospital-owned devices
  - PHI on devices? Remote access?
  - Policies regarding use
  - Limiting a users ability to download unapproved software
  - Ability to remotely wipe
  - Mobile Device Management software

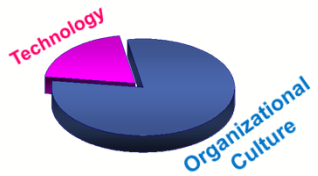
Other Items to Think About

- Inventory of where PHI resides
- Monitoring the monitors-remember Privileged Users
- ENCRYPTION
- Reporting line
- Sanctions for workforce who violate policies and procedures
  - –Communicating
  - –Applying consistently

Workforce Training

- Critical component of security program
- Targeted and repetitive
- Create understanding of real risks
- Lots of good training resources (commercial and free)
  - Caution – you might get what you pay for!

HIPAA Requires Culture Change



20% technical

80% policies & procedures

Questions?

Michael W. Chase
mchase@bairdholm.com
(402) 636-8326

Abigail T. Mohs
amohs@bairdholm.com
(402) 636-8296