INSIDER THREATS: HEALTHCARE PRIVACY & SECURITY

APRIL 16, 2018

INTRODUCTION – MICHELLE O'NEILL

Over 20 years of experience in health care administration, corporate compliance, physician contracting, and HIPAA privacy & security. Experience working for hospitals and physician practices. Currently working as the Director of Corporate Compliance and Privacy Officer for NJ's largest multi-specialty physician practice.

A LOOK BACK AT 2017…

HIPAA Enforcement Actions

- Memorial Healthcare System: $5.5M – Unauthorized employees had accessed the protected health information (name, SSNs, DOBs) of 115,143 individuals and disclosed it to an affiliated physician office staff.
- Children's Medical Center of Dallas: **$3.2M** – An unencrypted laptop was stolen from its premises. The laptop contained PHI for 2,462 patients.
- CardioNet: **$2.5** – 1st settlement involving a wireless health services provider. CardioNet provided remote mobile monitoring to patients at risk for cardiac arrhythmias. An unencrypted laptop was stolen and it contained data for 1,391 individuals.
- Memorial Hermann: **$2.4M** – A patient presented a fraudulent identification card to office staff at the clinic. Following the incident, Memorial Hermann issued a new release, which included the patient's name in the headline.
- Puerto Rico Life Insurance Company: **$2.2M** – A USB device, containing the PHI for 2,209 patients (name, DOBs, SSNs), was left in its IT department unguarded overnight and was stolen.
- Presence Health: **$475k** – Operating Room schedules went missing. The schedules contain the PHI for 836 patients, including names, birthdates, and types of procedures.
- Metro Community Provider Network: **$400k** – A hacker accessed employee email accounts and obtained 3,200 individual's PHI. An investigation found that the network failed to conduct a risk analysis.
- Mount Sinai St. Luke's : **$387k** – An employee inappropriately faxed a patient's PHI (containing his HIV status) to the patient's employer, rather than delivering it to the post office box.
- Center for Children's Digestive Health: **$31k** – Filefax stored records for the Center and the OCR found that there was no Business Associate Agreement on file.

CURRENT STATE OF HEALTHCARE PRIVACY & SECURITY

- 1st year of Trump Administration – Rocky for HHS
- New HHS OCR Director – Roger Severino sees his role as "shutting down the regulatory state." (OCR taking a lower profile in its enforcement & regulatory action)
- New privacy/security regulations not expected
- ONC Appoints New Chief Privacy Officer – Kathryn Marchesini

SCARY STATS

- ✓ The "2017 IT Risks Report" from Netwrix found that 100% of government workers surveyed saw their own employees as the most likely culprits during a security breach.
- ✓ The "2016 Cyber Security Intelligence Index, IBM" found that 60% of all attacks were carried out by insiders (¾ involved malicious intent, ¼ involved inadvertent actors); Research also found that health care was one of the top industries under attack.
- ✓ In 2016, Ponemon Institute found that 76% of IT Professionals stated that their organization experienced the loss or theft of company data and that the leading cause was insider negligence.
- ✓ Verizon's 2015 Data Breach Report found that Insiders are responsible for 90% of all Security Incidents (29% of Insider Threats were found to be deliberate and malicious and 71% were unintentional (misuse of systems, log-in/log out failures)

INSIDER THREAT

Either a malicious insider is going to intentionally exploit their access to your organizations data or a negligent worker is going to inadvertently expose it….this is considered an *Insider Threat.*

WHAT IS INSIDER THREAT?

Leaders put faith & trust in their judgement and intuition. We put faith in in the people that we hire and want to believe that they are loyal and put the organization's best interests first. At times, that trust is betrayed…

"Insider threat" is a generic term for a threat to an organization's security or information that comes from within. It is often used to refer to insiders maliciously or inadvertently using, damaging, or disclosing data.

Most breaches (despite the size or scope) are usually caused by an action or failure of someone INSIDE the organization.

TYPES OF INSIDER THREATS

- Accidental
- Negligent
- Malicious

ACCIDENTAL

According to Verizon's 2016 Data Breach Incident Report, accidents accounted for 20% of security incidents in 2015.

Why? -- Employees may not be educated enough on privacy/security best practices and/or employees make mistakes.

Examples:

- Clicking on a Phishing Email or Malicious Link -- Attackers are waiting for employees to make a mistake!
- Faxing to the Incorrect Party
- Email Accidents: One mistyped address can lead to a serious HIPAA Breach
- Faxing Accidents

NEGLIGENT

These are the inside threats where your employees do not pay attention to the policies that are in place to protect patient data. There is no malintent but they could open your organization up to dangerous security threats.

Examples:

- Leaving a PC unlocked
- Not sending secure emails – Emailing a patient spreadsheet to a personal email address to work from home

MALICIOUS

This is where individuals/employees inside your organization act "maliciously" as they may be motivated by financial gain or disgruntled.

Examples:

- A disgruntled employee may extract sensitive data and his/her way out and sell it on the black market or release it publicly.
- An employee may access friends or family members charts for curiosity and/or to do harm;
- A physician may be leaving your organization and starting up his/her own practice and may "steal" patient information lists
- An employee may sell information about a "high profile patient" to media outlets for financial gain
- Employees may post on social media patient information

THE DANGER OF *MALICIOUS* INSIDER THREATS

- **Insider threats can go undetected for years** – The longer you take to detect a breach, the more remediation costs go up. Insider threats can be tough to detect, which is why they are typically expensive to remediate.
- **It is hard to distinguish harmful actions from regular work** – This is what makes insider threats so hard to detect. When an employee is working with patient information, it is almost impossible to know whether they are doing something malicious (discuss examples);
- **It is easy for employees to cover their actions** – Any tech savvy employee will know how to clean up after themselves to conceal malicious action;
- **It is hard to prove guilt** – Even if you are able to detect a malicious action, employees can simply claim that they made a mistake and get away with it. It can be tough (or impossible, at times) to prove guilt (discuss examples);

THE CAUSE OF *MALICIOUS* INSIDER THREATS

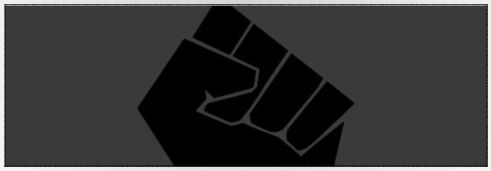
- **Opportunity** – An employee sees an opportunity to use patient information for personal gain or to steal it, or sell it.
- **Revenge** – Disgruntled employees can steal patient information, leak it online, or damage it to get back at your organization.
- **Political/Social Statements** – Some employees misuse your organization's patient information (leaking data online or damaging it) to make a political or social statement (think about Edward Snowden, who leaked employer's data in order to protest government surveillance).
- **Future Competition** – Employees may want to start up their own practice and decide to steal your patient information to contact patients.
- **Curiosity** – Employees may misuse patient information to gain information that they are curious about (family drama, high profile patients, fellow employees).

WHO SHOULD YOU PAY CLOSEST ATTENTION TO

- Privileged Users: These individuals are typically the most trusted users in your organization but they have the most opportunities to do harm, both intentionally and unintentionally.
- Third Parties: Employees working remotely, subcontractors, vendors also have access to your systems. There is often less ability to oversee and you don't always have a relationship with them, nor do they go through the organization's training. They are a security risk.
- Terminated Employees: Employees may decide to take data with them when they are terminated. If there are not clear policies regarding termination procedures in place, they may still be able to access upon termination.

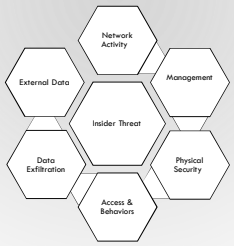
ARE YOUR EMPLOYEES BEING RECRUITED BY CYBER CRIMINALS???

- The dark web market for stolen PHI and PII is massive, with some estimates claiming that it is worth around $120 billion;
- Cyber criminals are recruiting employees to assist in collecting patient information;
- A recent McAfee report specifically states that the healthcare industry is a major target



HOW TO FIGHT BACK AGAINST INSIDER THREATS

BE ON THE LOOKOUT!!!



IMPLEMENT AN "INSIDER THREAT MITIGATION PROGRAM"

- ✓ **Proactively Detect Individuals Who May Pose a Potential Insider Threat**
- ✓ **Raise Awareness**
- ✓ **Mitigate Threats and/or Damages**

KNOW AND MANAGE YOUR EMPLOYEES

- ✓ **Background Checks** – The recommendation is to include financial checks
- ✓ **Watch Employee Behavior** – Pay close attention if your employee is unhappy/disgruntled. Look at changes in employee behavior and/or monetary situation. Watch changes in hours worked (coming in very early, staying very late).
- *51% of employees involved in an insider threat incident had a history of violating IT/Compliance policies leading up to the incident*
- *92% of insider threat cases were preceded by a negative work event, such as termination, demotion, or a dispute with a supervisor*

"Insider Threats: What every government agency should know and do," Deloitte Dbriefs, March 2016

USE THE PRINCIPLE OF LEAST PRIVILEGE

- ✓ Cyber Security standard …The fewer privileged employees you have, the easier it is to protect your patients' information
- ✓ Fewer employees can conduct malicious actions, fewer accounts can be hacked into, fewer mistakes can happen.
- ✓ Also applies to 3rd parties (temporary credentials is a good solution to 3rd parties).

MONITOR YOUR EMPLOYEES/USERS

- ✓ **Control User Access** –Use unique complex passwords that are not shared; Use two-factor authentication.
- ✓ **Monitor User Actions** – Do proactive audits (monitor for suspicious activity); Do behavioral monitoring (accessing remotely, outside of normal business hours, or both); Review failed remote login attempts (especially those that occur at odd times). If possible, engage with a security monitoring company

HAVE SOLID TERMINATION PROCEDURES IN PLACE

✓ Access Disabled – Physical and System Access

✓ Exit Interview

- *90% of IT employees indicate that if they lost their jobs, they'd take sensitive data with them*
- *59% of employees who leave an organization voluntarily or involuntarily say they take sensitive data with them*

"Insider Threats: What every government agency should know and do," Deloitte Dbriefs, March 2016

TRAINING

✓ Employees need to be aware of the privacy and security policies and procedures and know what the consequences are of not following them. Arm your employees and make sure that they are an asset to your security, not a liability. Empower them. Host phishing campaigns; Discuss physical security; Empower your employees to report concerns to you – See something, Say something!

✓ Make sure your employees are well aware of the consequences of violating your organizations privacy/security policies and procedures.

KNOW ALL OF YOUR USERS (NOT JUST YOUR EMPLOYEES)

✓ Know all users - Business Associates/Trusted Business Partners/Contractors

✓ Outline Guidelines & Hold Them Accountable

✓ Monitor Their Use, As Well

✓ Make Sure BAAs are signed

✓ Distribute BAA Best Practices Guide

✓ Send Annual Compliance Checklist

✓ Have BAs, partners, contractors, etc. sign a user confidentiality agreement

✓ Have process in place (e.g., User Request form with approvals)

MAKE SECURITY PART OF YOUR ORGANIZATION'S CULTURE

- ✓Make security a priority across your organization.
- ✓Send out Reminders/Tips
- ✓Corporate Compliance Week – Use this week to remind staff of your program
- ✓Reviews/Retraining with Staff – not just upon hire/annually & identify your high risk areas/users

REFERENCES

"Insider Threats: What every government agency should know and do," Deloitte Dbriefs, March 2016

Verizon 2015 Data Breach Investigation Report

Verizon 2016 Data Breach Investigation Report

Insider Threats as the Main Security Threat in 2017, Trapwire Guest Authors, 4/11/17

The Biggest Cybersecurity Threats are Inside Your Company, Mark van Zadelhoff, 9/19/16

QUESTIONS