



Security Breaches



Goal

- 1** To describe the risks and types of breaches that healthcare providers are encountering.
- 2** Simulate an IT security incident and develop tactics for addressing.



Current Situation

- Breaches occurring with frequency
- Cyber-attacks have been monetized
- Workforce is a risk
- Incident preparedness is a challenge
- Office of Civil Rights conducting audits
- Challenges continue to evolve



Agenda

1 Breaches & Risks

2 Mini Table Top Exercise

3 Wrap-Up



Takeaways

- Increase awareness of breaches
- Appreciate the need for practice
- Recognize the non-IT aspects



Breaches

“A **data breach** is the intentional or unintentional release of secure or private/confidential information to an untrusted environment.”

Breaches

HIPAA

“A breach is, generally, an impermissible use or disclosure under the Privacy Rule that **compromises the security or privacy of the protected health information.** An impermissible use or disclosure of protected health information is **presumed to be a breach** unless the covered entity or business associate, as applicable, **demonstrates that there is a low probability** that the protected health information has been compromised based on a risk assessment.....”

In the News

Advocate Health Care to pay \$5.6 million for potential HIPAA violations, the largest settlement yet for a single entity

OCR found the Illinois-based health system failed to conduct a thorough risk assessment and limit physical access to electronic health systems, among other infractions.

By [Jessica Davis](#) | August 04, 2016 | 03:22 PM

SHARE 104



Privacy & Security

Delaware oncology group hit by nearly month-long ransomware attack

Medical Oncology Hematology Consultants discovered the cyberattack on July 7, which may have breached the records of over 19,000 patients.

By [Jessica Davis](#) | September 01, 2017 | 10:38 AM



Privacy & Security

5 months after phishing attack, AU Medical reports potential breach

While officials say less than 1 percent of patients impacted by the breach, this is the second organization has been hit with a successful breach within the last year.

By [Jessica Davis](#) | September 18, 2017 | 02:34 PM

Privacy & Security

106,000 patient records potentially breached by 3rd-party vendor

The computer system of the Radiology Center from Mid-Michigan Physicians Imaging Center was breached in March, but officials say the extensive investigation delayed the breach.

By [Jessica Davis](#) | August 30, 2017 | 02:05 PM



Compliance & Legal

Nationwide pays \$5.5 million for 2012 breach of 1.27 million accounts

The insurance company settled with 33 states for failing to patch a vulnerability that allowed a hacker to gain access to its system.

By [Jessica Davis](#) | August 11, 2017 | 02:32 PM



Phishing attack at Colorado Mental Health Institute impacts 650 patients

The state has been unable to determine whether breached information was seen by a third party, but officials said names, dates of birth and Social Security numbers may have been compromised.

By [Mike Miliard](#) | December 26, 2017 | 12:52 PM



Privacy & Security

San Antonio's largest OB-GYN provider breached by keylogger malware

Hackers spent one month on the servers of The Institute for Women's Health, stealing both financial and personal health data.

July 05, 2016

Nursing home operator to pay \$650,000 after cell phone with patient records stolen



Share this content:

A stolen iPhone containing the medical records of more than 400 nursing home patients will cost the former owner of several nursing homes \$650,000 under a federal settlement.

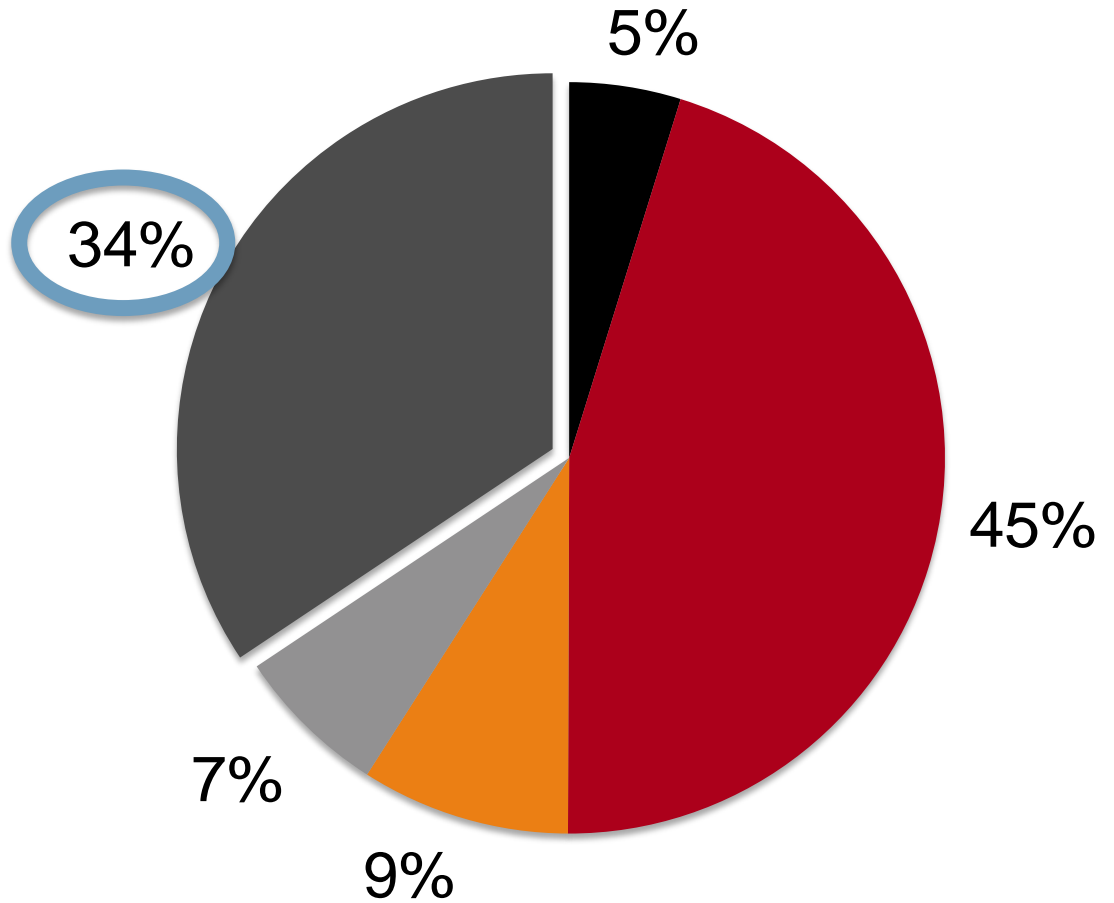


Breaches

SOURCES

Percentage of Breaches

- Banking
- Business
- Educational
- Government/Military
- Healthcare



Breaches

COST

COST EXAMPLES

- Investigation
- Remediation
- Identity monitoring
- Reputational
- Lost customers
- Equipment
- Legal
- Public relations

AVERAGE¹

\$225 per record

HEALTHCARE¹

\$380 per record



Breaches

WHAT CAUSES
THEM?

COMMON FACTORS

- Insider access/curiosity
- User carelessness
- Weak passwords
- Application and hardware vulnerabilities
- Elevated privileges
- Phishing

IMPACT OF
THREAT



LIKELIHOOD OF
OCCURRENCE

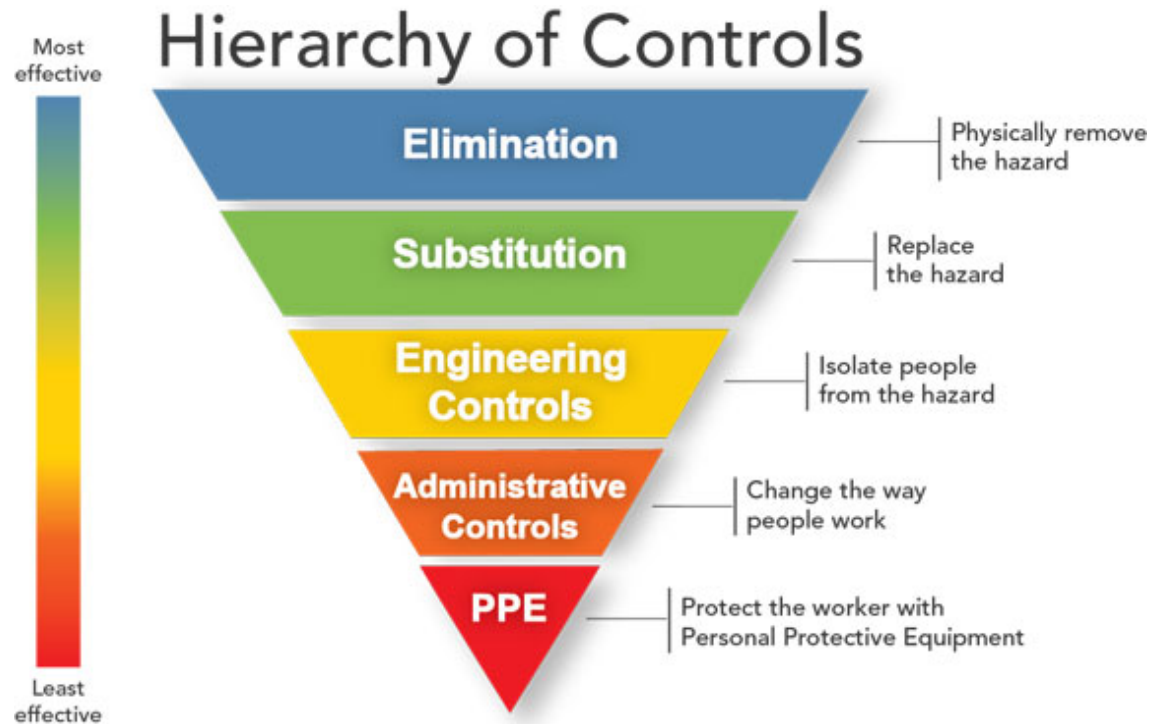


RISK



IT Risk

Controls are applied to identified risks to reduce the likelihood and impact





Ten Risks

1. The Internet of Things (IoT)
2. Network Secured Only At Perimeter
3. The World of Fakes
4. Smartphone Hacking
5. Mergers and Acquisitions
6. Government Hacking
7. Cyber Insurance
8. Phishing
9. Lacking Risk Assessments
10. Ransomware



Five Added Factors

SENIOR LIVING ORGANIZATIONS:

1. High staff turnover
2. Increased EHR usage
3. Small or no IT teams
4. Geographic span
5. Increasingly mobile staff

OCR

HIPAA AUDITS

- OCR has completed over 200 desk audits
- Onsite audits begin in 2017 – 2018



DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE OF THE SECRETARY

Voice – (202) 619-0403 TDD – (202) 619-2357 FAX – (202) 619-3818
<http://www.hhs.gov/ocr>

Office for Civil Rights
200 Independence Ave., SW; RM 509F
Washington, DC 20201

Name of Entity

Address of Entity

Point of Contact of Entity

Dear Covered Entity:

The Office for Civil Rights (OCR) of the Department of Health and Human Services (HHS) has responsibility for administration and enforcement of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules (45 CFR Part 160 and Part 164 Subparts C and E). These rules are designed to provide important health information privacy and security protections and rights for individuals. The OCR is committed to developing and enforcing strong health information privacy protections that do not impede access to quality health care.

The American Recovery and Reinvestment Act of 2009 (ARRA) requires HHS to audit covered entity and business associate compliance with the HIPAA privacy and security standards. To effectively implement this statutory mandate, OCR has engaged the services of a professional public accounting firm (BerryDunn) to conduct performance audits, using generally accepted government auditing standards. You are receiving this letter because OCR has selected [Name of entity] to be the subject of an audit.



OCR

HIPAA AUDITS

OCR FINDINGS THUS FAR:

- Risk analysis
- Risk management
- Business associate agreements
- Transmission security
- Auditing
- Software patching
- Media disposal
- Backup and contingency planning




What Can You Do?

1. Conduct a risk assessment.
2. Do the basics really well.
3. Develop an incident response plan.
4. Increase workforce awareness.
5. Revisit your disaster recovery plans.
6. Coordinate with your vendors.
7. Conduct table top exercises.

Mini Table-Top





Who are you?

1. Each table in the room is the management team of Cyber Acres.
2. Cyber Acres is a 5 community organization with IL, AL, and SNF services.
3. You have 2 IT people and then contract with an outside support vendor.
4. You have a central office team and also staff at the specific communities in the areas of finance, payroll, and HR.

Fact 1

While sitting at your weekly management meeting your director of revenue cycle mentions that they have received emails from 4 of the 5 business office managers describing unusual system slowness when generating bills and preparing payroll.

All of the business office managers are blaming your IT person for upgrading the system last night.



Fact 1

WHAT QUESTIONS DO YOU HAVE?

WHO DO YOU INVOLVE?

WHAT DO YOU DO?

Fact 2

After leaving the meeting you ask your IT Team to look into the slowness.

After an hour, your IT person describes that he has found malicious software running on a few of your servers.

These servers host your EHR, billing, and payroll software including the software that the business officer managers were complaining about.



Fact 2

WHAT QUESTIONS DO YOU HAVE?

WHO DO YOU INVOLVE?

WHAT DO YOU DO?



Fact 3

After calling your IT support vendor and troubleshooting the server, your IT team lets you know that the malicious software is ransomware and your core systems are currently encrypted and data cannot be read by any end-users.



Fact 3

WHAT QUESTIONS DO YOU HAVE?

WHO DO YOU INVOLVE?

WHAT DO YOU DO?



Conclusion

Your IT team and support vendor were able to confirm that your backup was not affected by the ransomware and was able to restore your systems from the 3 am backup.

Your team takes the team out to dinner to celebrate!

Mini Table-Top



Fact 1

Your IT person, joyous from the triumphant recovery from ransomware but shaken from the stress of the situation decides to make an extra backup of your systems to take offsite to one of your locations the next day.

On his drive home he stops at Hannaford to pick up something for dinner.

Upon returning to his car he finds his windows broken and his laptop bag gone.



Fact 1

WHAT QUESTIONS DO YOU HAVE?

WHO DO YOU INVOLVE?

WHAT DO YOU DO?



Conclusion

Your IT person used the encryption software you use to manage your devices and USB drives.

He encrypted the external hard drive he used for the backup to prevent unauthorized access to the data it contained.



Conclusion

AGENDA

1. Breaches and Risks
2. Mini Table Top Exercise
3. Wrap Up

TAKEAWAYS

- Increase awareness of breaches
- Appreciate the need for practice
- Recognize the non-IT aspects