Insider Threats

Types of Insider Threats

Negligent or Unintentional

Example
An employee responds to a phishing email and provides credentials.

How to Protect
- Regular staff training & education
- Phishing assessments

Malicious

Example
An employee accesses thousands of health records in order to sell the information they contain.

How to Protect
- Limit user access to only what is necessary for role

Intentional, Non-Malicious

Example
A doctor copies patient records to market a new business to previous patients.

How to Protect
- Proactive privacy monitoring
- Regular staff training & education

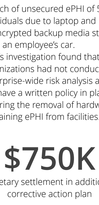
> The fact that someone looks at information four times the frequency that their neighbor does—the fact that an individual is looking at four times as many records, is absolutely a flag. They're either working four times as hard/fast, or are snooping, or are engaged in nefarious activities.
>
> *– Mac McMillan, CEO, CynergisTek, Inc.*

Insider Breaches

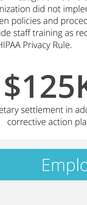
Negligent and Malicious Behaviors of Most Concern to Organizations

- Unleashing Malware from an Insecure Website or Mobile Device
- Violating Access Rights
- Using Unapproved Mobile Device in the Workplace
- Use of Unapproved Cloud or Mobile Apps in the Workplace
- Accessing Company Applications from an Insecure Public Network
- Succumbing to a Phishing Attack

Data Breach Root Causes



Did your organization have a security incident or data breach due to a malicious or negligent employee?



28% of employees admit that they have uploaded a file containing sensitive data to the cloud.

According to a study funded by the U.S. DHS, insider threats can go undetected for an average of

32 months

OCR Settlements Due to Insider Breaches

Cancer Care Group

- Breach of unsecured ePHI of 55,000 individuals due to laptop and unencrypted backup media stolen from an employee's car.
- OCR's investigation found that the organizations had not conducted an enterprise-wide risk analysis and did not have a written policy in place covering the removal of hardware containing ePHI from facilities.

$750K
Monetary settlement in addition to corrective action plan

Parkview Health System, Inc.

- Breach of 5,000 to 8,000 patients' medical records that were left unattended in cardboard boxes in a physician's driveway.
- The settlement includes a requirement that the organization update their policies and procedures and train staff.

$800K
Monetary settlement in addition to corrective action plan

Cornell Prescription Pharmacy

- Breach of 1,610 patients' PHI due to improper disposal of documents, which were found in an unlocked, open container on the organization's premises.
- OCR's investigation found that the organization did not implement any written policies and procedures or provide staff training as required by the HIPAA Privacy Rule.

$125K
Monetary settlement in addition to corrective action plan

Concentra Health Services

- Breach of unsecured ePHI due to an unencrypted laptop stolen from one of the organization's facilities.
- OCR's investigation found that the organization had discovered in its own risk analyses that unencrypted devices were a critical risk but had not taken complete or consistent action to mitigate that risk.

$1.7M
Monetary settlement in addition to corrective action plan

Employee Security Training

How would you grade the effectiveness of your security training and awareness activities for your organization's staff members and physicians?

Only **31%** of respondents rated the effectiveness of their security training and awareness activities as "very good" or "excellent".

> Well-informed users make fewer mistakes, so turn up the education and don't forget to make it interesting and relevant.
>
> *– Mac McMillan*
> *CEO, CynergisTek, Inc.*

What Best Describes the Structure of Your Organization's Data Protection and Privacy Training Program?

Learn how to reduce the insider threat at your organization: http://cynergistek.com/privacy/

CynergisTek, Inc. 512.402.8550 info@cynergistek.com
cynergistek.com @CynergisTek

Sources

"Cybersecurity: Things Are Getting Worse, But Need to Get Better, Says Mac McMillan" - *Healthcare Informatics*: http://www.healthcare-informatics.com/article/cybersecurity-things-are-getting-worse-need-get-better-says-mac-mcmillan

"Managing Insider Risk through Training & Culture" - *Ponemon Institute*: https://iapp.org/media/presentations/13Summit/S13_Lessons_Learned_OCR_PPT.pdf

"Protecting Your Network From Hackers" - *Health IT Outcomes*: http://www.healthitoutcomes.com/doc/protecting-your-network-from-hackers-0001

"2015 Healthcare Information Security Today Survey" - *ISMG*: http://www.healthcareinfosecurity.com/surveys/whats-state-health-information-security-s-32

"Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data" - *Ponemon Institute*: https://www2.idexpertscorp.com/sixth-annual-ponemon-benchmark-study-on-privacy-security-of-healthcare-data-incidents

"Safeguarding against insider security threats" - *Healthcare IT News*: http://www.healthcareitnews.com/news/safeguarding-against-insider-security-threats

"Humans: Still the weakest link in the enterprise data security posture" - *Data on the Edge*: http://www.healthcareitnews.com/news/safeguarding-against-insider-security-threats