Breach Avoidance

The Only Meaningful Safe Harbor Strategy

Mac McMillan
CEO CynergisTek, Inc.
Chair HIMSS Privacy & Security Committee
NIST/OCR HIPAA Security Rule Conference
Washington, D.C. May 10/11, 2011

Speaker's Background

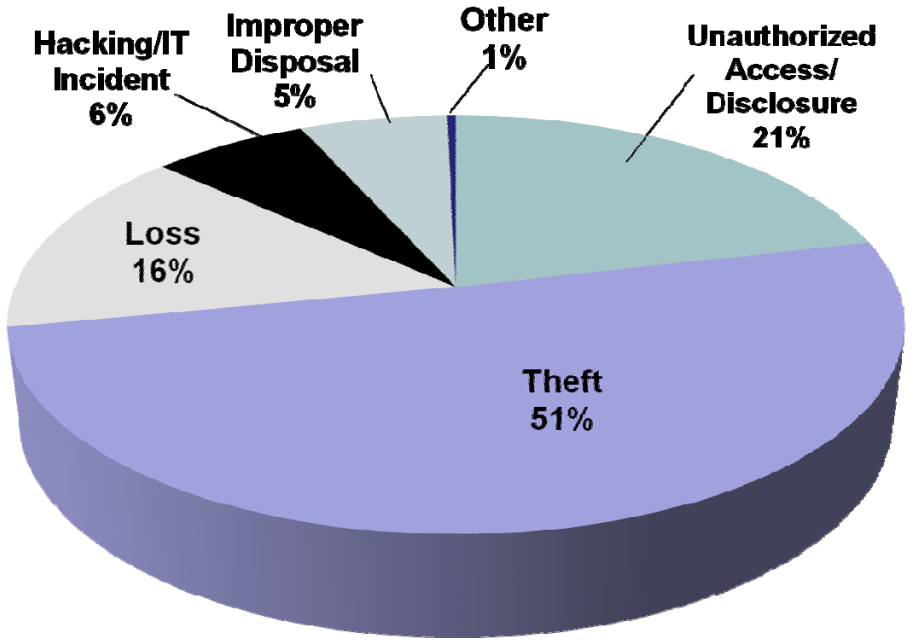
- Founder & CEO CynergisTek, Inc.
- Chair, HIMSS Privacy & Security Committee
- Former Chair HIMSS Information Security Work Group
- Advisory Board Member Diebold Healthcare Solutions
- Editorial Advisory Board, Health IT Security
- Contributing Author HIMSS Book, *Information Security in Healthcare: Managing Risk*
- Director of Security, Defense Threat Reduction Agency
- Retired Intelligence Officer, U. S. Marine Corps

Discussion Outline

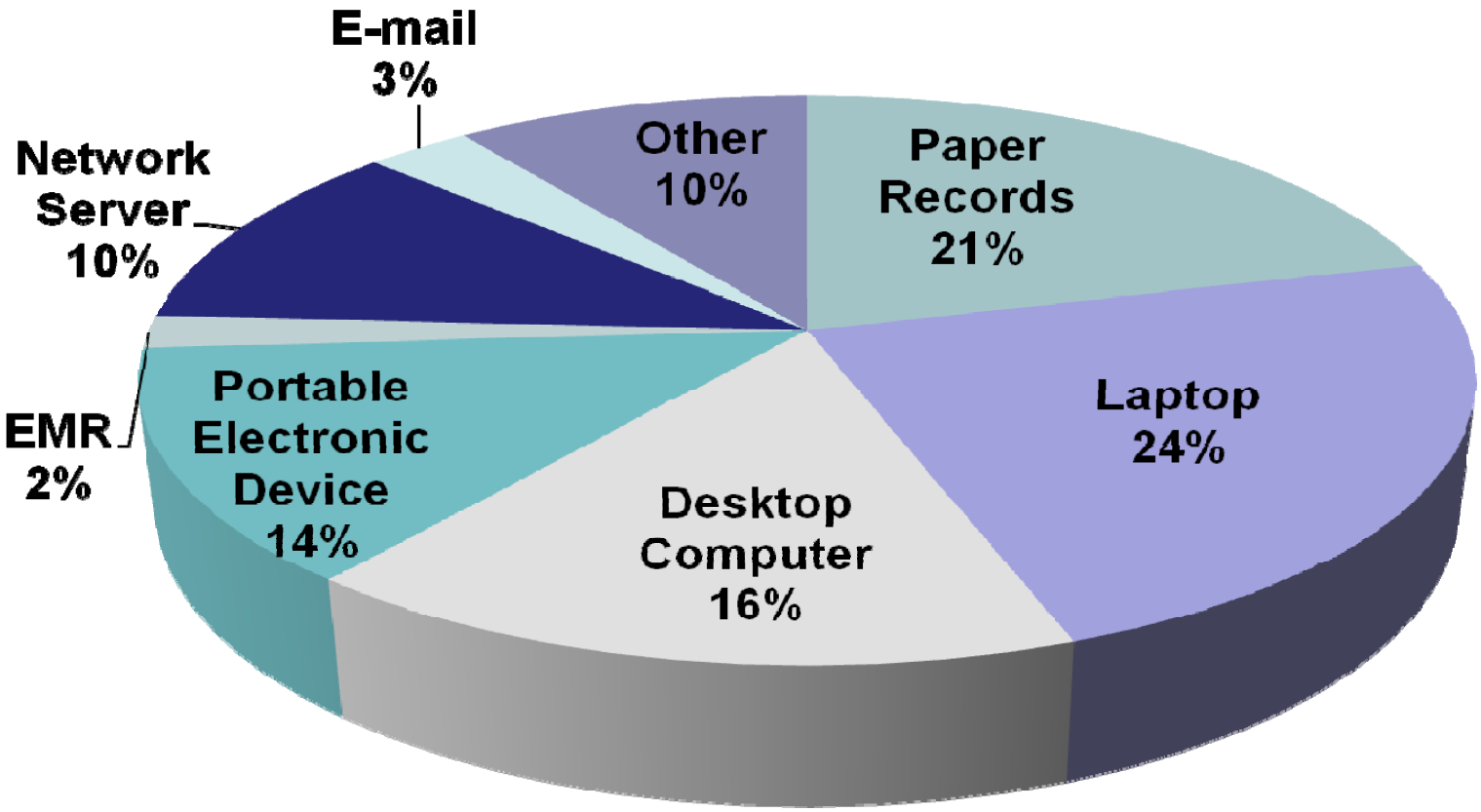
- A Quick Reminder: Why We're Discussing This Topic
- Encryption Is An Option, Not A Mandate
- Re-Evaluating Our Enterprise Security Standard
- Making Safe Harbor Meaningful

Why Are We Talking About This?

- 240 + Major breaches in 2010
- Approximately 31,000 Smaller breaches
- 67% Due to loss/theft of unencrypted devices
- Far less than half encrypt data a rest
- Nearly 30% don’t encrypt email
- Many mobile devices, phones, pads, thumb drives remain unencrypted
- Less than 20% employ DLP



Primary Offenders



Is Safe Harbor Our Best Choice?

- Safe Harbor is achieved by rendering PHI unreadable, indecipherable, unusable by anyone other than those authorized.
- Safe Harbor is achieved by employing appropriate encryption of “unsecured” PHI data.
- Safe Harbor can also be achieved through appropriate destruction, or…
- We can manage our data through a better integrated set of controls and reduce the risk of exposure to breach.

The Rules Have Not Changed

The Breach Notification Rule does not modify responsibilities under the HIPAA Security Rule nor does it impose new requirements to encrypt “all” protected health information. Entities are permitted to use “any” security measure that allows them to reasonably and appropriately implement safeguards.

HIPAA / HITECH

So neither HIPAA nor HITECH nor the Breach Notification Rule take away a CE's flexibility in addressing how it safeguards protected health information or requires encryption.

- Breach of PHI without reasonable protection - HIPAA Security Rule issue
- Breach of PHI without appropriate encryption - Notification issue

Re-evaluating The Enterprise

To be most effective, an information security strategy needs to address more than just encryption. It should include encryption as one element of an integrated approach that “uses” all reasonable and appropriate safeguards to manage the risk effectively. Encryption should not necessarily be our first choice for mitigating the risk of breach and Safe Harbor should be result of our efforts not the desired End State.

The Reasons Are Simple

- Encryption is not a complete solution,
- Can eliminate flexibility,
- Requires maintenance and administration,
- Can impact performance and user workflows,
- Is not yet feasible everywhere,
- Is costly to maintain (versions), and
- Does not address appropriateness

Step One: Manage Patient Information Smartly

- Discover where critical data is in the enterprise, utilize an appropriate discovery tool
- Map data life cycle & workflow requirements where appropriate
- Determine where data “needs” to be accessible and how
- Don’t let data manage the solution

Step Two: Use Architecture to Segment/Isolate

- Data sources should only be accessible where necessary and to whom necessary.
- Reduce or eliminate access to data sources to reduce and eliminate risk.
- Deploy true segmentation through application firewalls / Access Control Lists.
- Deploy separation in networks where appropriate.

Step Three: Use Network Controls to Restrict Access

- Network integrity is a critical component of data security and encryption relies on it.
- Deploy Network Access Controls (NAC) solutions to block rogue or compromised system access.
- Conduct ongoing vulnerability analysis and remediation to mitigate potential for breach.
- Use IDS/IPS to detect rogue attempts to connect and malicious behavior.
- Ensure anti virus protections are up to date, deployed throughout and scan frequently

Step Four: Address Unique System Control Requirements

- Identify the universe of systems and applications with PHI.
- Use configuration as a means to eliminate or reduce risk, by hardening and locking down systems through group rules.
- Identify all reasonable options for avoiding local storage of sensitive information.
- Focus on eliminating, restricting or controlling access.

Multiple Options Exist:

- Virtualization of systems, particularly desk tops, laptops, pads, etc.
- Applying Group Policy to lock systems
- Disabling/enabling services/functionality
- Client computing, Citrix/Terminal Service for remote access
- Time outs for applications/systems
- Implementing Limited Data Set where available

Step Five: Implement Supplemental Technologies & Controls

- Architecture, network and organic system controls will only get us so far…
- Supplemental technologies monitor, enforce and enhance network & system controls
- Network Access Control, Intrusion Detection Systems, Data Loss Prevention
- Configuration Managers, Log Managers, Data Base Auditors, SIEM, etc.

Step Six: Apply Encryption to Fill Gaps

- Consider encryption requirements throughout the enterprise.
- Consider encryption in any circumstance where the risk to PHI cannot be reasonably eliminated.
- Avoid (User) decision based solutions that rely on policy.
- Encrypt mobile devices with PHI, regardless of other measures deployed
- Encrypt data in motion, everywhere

Step Seven: Address Physical Security Integration

- Physical controls such as access controls, alarms, cameras, etc. complement security for fixed assets.
- Physical controls compensate for lack of controls on certain devices such as printers, copiers, modalities, and devices that cannot be secured adequately.
- Deploy asset tracking solutions to aid recovery/investigation, and remote wipe options to eliminate risk of compromise.

Step Eight: Ensure Audit & Monitoring of Controls

- Utilize log monitoring to manage controls, audit user actions (Network/Application).
- Take advantage of audit capabilities in other technologies; DLP, Network Monitors, email encryption, vulnerability scanners, etc.
- Conduct process and controls audits where automation is not possible.
- Develop a SIEM strategy to enhance content based awareness and decision making.

Step Nine: Security Awareness & User Training

- “They” are the weakest link!
- Establish clear policies around data security and incident response.
- Train users according to their role and needs.
- Start at orientation and reinforce frequently.
- Regularly monitor user actions.
- Clearly define sanctions and responsibility.

Step Ten: Options for Transferring Risk

- Notice I did not say “responsibility”.
- The reality is that risk cannot be totally eliminated, and encryption, while it may avoid notification, is not a foolproof solution.
- Outsourcing, such as using SAAS or an ASP solution can transfer part of the risk; BAA considerations are important.
- Cyber Insurance can also provide additional mitigation in times of breach.

Wrapping It Up

- Safe Harbor is a concept discussed in HITECH under the Breach Notification Rule
- Safe Harbor is achieved through employing appropriate encryption technologies or through proper destruction
- HITECH does not modify or change the intent of the encryption requirement under HIPAA
- Entities can and should consider all reasonable controls to protect health information
- However, the focus should be on avoiding breaches, not just notification.

Questions