

Microsoft HUG Tech Forum

Saturday, April 4, 2009

MEDICAL RECORDS ARE AT RISK!

Ali Pabrai, CISSP (ISSAP, ISSMP), CSCS
ecfirst, Chief Executive



ecfirst's HIPAA compliance training have the exclusive endorsement of the AHA

The Human Body



- **Most studied subject of all times**
 - 10 trillion cells in our body
 - 70 million cell replications every day – we are busy!
 - The brain is arguably the most complex structure in the universe
 - Our brain has about 100 billion nerve cells
 - The brain loses about 40,000 nerve cells every day
- **Blueprint of life – Our Genes!**
 - Language in which God created life – Bill Clinton, June 26, 2000
 - Genes shape our lives, carried in our chromosomes
 - Full sequence of human genome consists of 6 billion DNA letters that make up thousands of genes (26,588) strung around 46 chromosomes

Journey from intuitive medicine toward precision medicine has begun

The Innovator's Prescription, Christensen

State of American Healthcare

- **Healthcare in America Today** (Source: WSJ – Feb 24, 2009)
 - American healthcare expenses are expected to reach **\$2.510 Trillion**
 - U.S. government healthcare expenditure is expected to reach \$1.191 Trillion
 - Private sector expenditure is expected to be \$1.319 Trillion
- **Healthcare Information Technology in America**
 - Too many servers, too many applications
 - Too many credentials across multiple systems to manage
 - Too many PCs to support and maintain
 - Mobility of devices is rapidly increasing
 - Storage demands are rising fast
 - Highly specialized technical skills required
 - Serious lack of redundancy in infrastructure
 - Struggle with resources to monitor and audit

Is Your Organization Next?

- **Harris County Hospital, Texas** – *Administrator lost medical/financial records of 1,200 patients with HIV/AIDS – Information was on a portable flash drive – Data was not password protected nor encrypted*
- **Staten Island University Hospital, NY** – *Computer with Medical Records Stolen - Patients informed 4 months later*
- **UCSF Medical Center** – *Information on patients was accessible on the Internet - Patients informed 6 months later*
- **New York-Presbyterian Hospital/Weill Cornell Medical Center** – *2000 patient records sold; 50,000 improperly accessed*
- **University of Utah Health Care** – *Password protected but unencrypted laptop with data on 4,800 people was stolen after hours from a locked room*
- **University of Minnesota Reproductive Medicine Center** – *Doctor lost an unencrypted portable storage device with information on 3,100 patients*

Recently, the VA agreed to pay \$20 Million to settle a class action lawsuit over the 2006 loss of a laptop containing personal information on up to 26.5 million veterans

Medical Identity Theft

A Rising Risk

The Perpetrator vs. the Victim

- 249,000 had their medical identities stolen in 2005
 - Gartner Research estimates more than 1 million cases of medical identity theft in 2008
- Two areas of vulnerability:
 - Use of a person's name or identifiers without knowledge or consent
 - Use of a person's identity to obtain money by falsifying claims for medical services
- FACTA regulation includes provisions to reduce identity theft
 - Mandatory deadline – May 1, 2009
 - Has your organization complied with the Red Flag and Address Discrepancy Rules?
 - Need to develop an Identity Theft Prevention Program

Information - The New Currency of Business

Global State of Information Security – PWC Report 2008

- Most organizations do not know where their most important data is located
- From protecting privacy to improving safeguards – organizations are struggling
- Greatest risk to sensitive corporate information is that a user with either legitimate or unauthorized access will compromise data – intentionally or accidentally
- Data breaches are really damaging
 - Financial losses, Theft of IP, Compromise of brand, Fraud
- Nearly 50% of respondents can't identify vulnerabilities that led to security incidents!
- Employees & former employees remain biggest threat!

What is the risk to information assets?

How confident are you about your organization's information security posture?

Providence, CVS & Beyond

The Launch of Audits: OCR, OIG, CMS, FTC

Providence

- Media and laptops lost or stolen with PHI of over 386,000 patients
- HHS received over 30 complaints
- OCR and CMS focused their investigations on Providence's failure to implement policies and procedures to safeguard PHI
- Resolution Agreement and Corrective Action Plan executed to settle potential HIPAA violations
- Fined \$100,000 and must submit compliance reports for a period of 3 years

CVS

- Failed to implement policies and training for disposal of PHI
- Was investigated by OCR and the FTC
- HHS and FTC require CVS to actively monitor its compliance with the Resolution Agreement and FTC Consent Order
- Fined \$2.25 Million and follow HHS Corrective Action Plan for 3 years
 - FTC requires monitoring for 20 years

Ready for a CMS Audit?

HIPAA is the Floor

When Were These Documents Last Updated?

- Entity-wide security plan
- Risk analysis (most recent)
- Vulnerability scanning plans
- Network penetration testing policy and procedure
- List of all user accounts with access to systems which store, transmit, or access EPHI
- Encryption or equivalent measures implemented on systems that store, transmit, or access EPHI
- Data backup procedures, disaster recovery plan including test plans and results

HITECH Act & State Regulations

Beyond HIPAA Privacy | Security

- **Health Information Technology for Economic and Clinical Health (HITECH)**
 - Privacy and Security Breach Notification to Individuals
 - Business Associates = Covered Entities?
 - New Penalties Defined
 - Personal Health Record Vendors – Now Covered!
- **SB 1386** - notification of security breaches involving “unencrypted” sensitive data
- **AB 1950** - organizations take “reasonable precautions” to protect CA residents’ personal data from modification, deletion, disclosure, and misuse
- **AB 1298** - expands data breach notification law to include unencrypted medical histories, health insurance information, medical treatments & diagnoses
- **SB 541** - breaches must be disclosed to the affected patients within 5 days
- **AB 211** - fines starting from \$2,500 to \$25,000 per violation for organizations that negligently disclose patient records

Where Are We Headed in 2009?

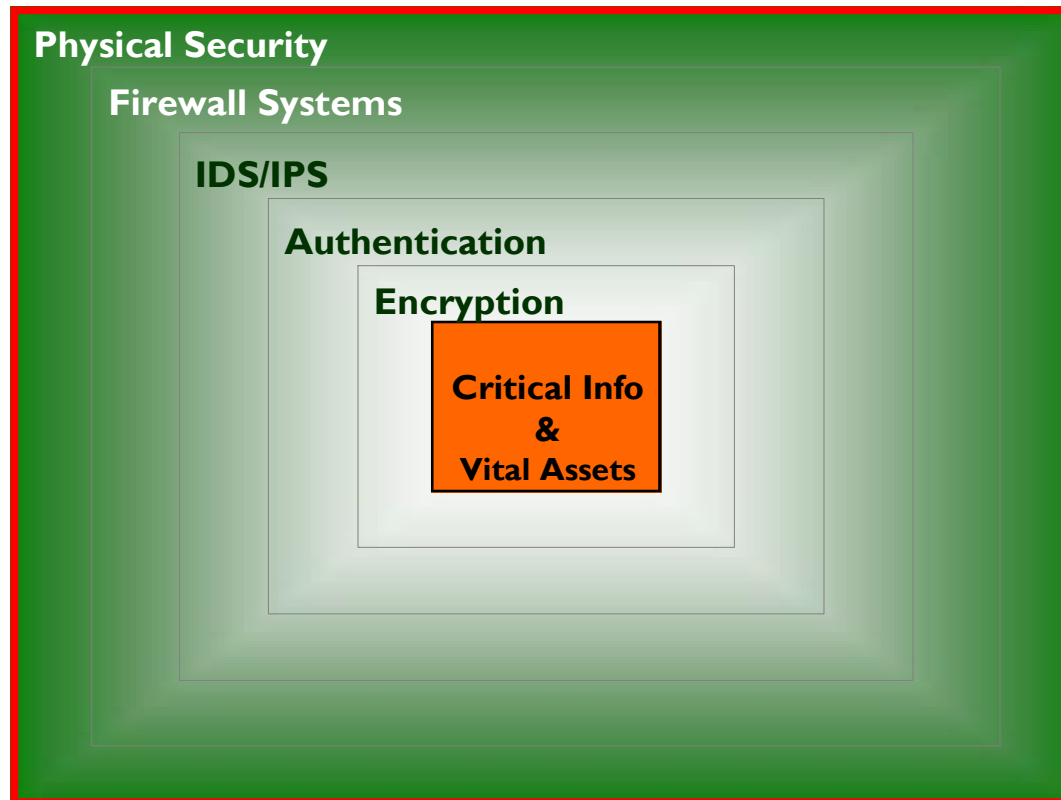
- “Thin is In”
- Bring the complexity to the data center
- Reduce the number of servers
 - Virtualization
 - Blade servers
- Plan for multi-tier storage architecture
- Bake in security:
 - Compliance
 - Redundancy
- Focus on security appliances, simplify maintenance and support

Emerging Security Best Practices

- Harden Firewall Solutions, IDS/IPS
 - What is your DMZ Architecture?
- Secure Facilities & Server Systems
 - How Secure is your Data Center?
- Implement Identity Management Systems
 - Single Sign-On (SSO) is Increasingly a Requirement
- Schedule Regular Scans of the Infrastructure
 - Have you Identified your Vulnerabilities?
- Develop Contingency Plans
 - Alternate Data Center Ready & Tested?
- Update Security Policies
 - Approved by Management, Communicated to Employees?
- Encryption is Key!
 - Laptops, backup media, removable media, database servers

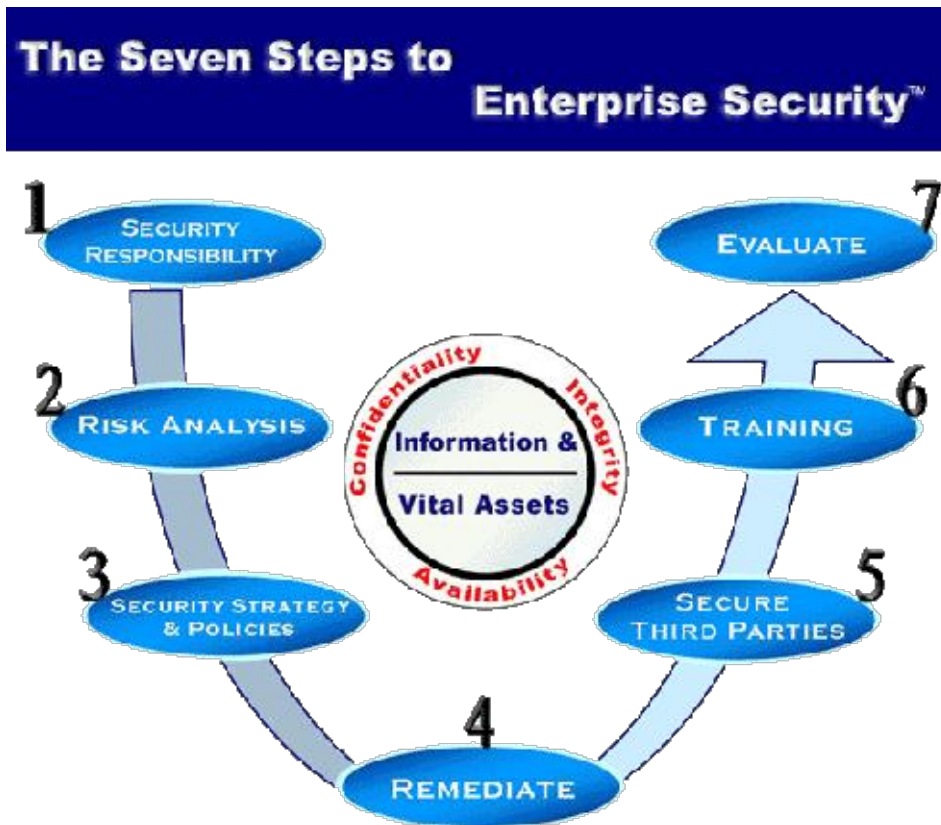
An Information Security Program

Strategy: Edge to Core



Study the ISO 27000 Security Series!

Medical Records Are At Risk!



What are your security controls?

Pabrai's Laws of Information Security

Is Your Security Kismet or Karma?

1. There is no such thing as a 100% secure environment
2. Security is only as strong as your weakest link
3. Security defenses must be integrated and include *robust* (passive) and *roving* (active) controls to ensure a *resilient* enterprise
4. Security *incidents* provide the foundation for security *intelligence*

Is Your Security?

Kismet – A Reactive Security Framework

Karma – A Proactive Security Framework

Source: **Cyber Security Strategy**, Ali Pabrai, www.ecfirst.com

The Next 10 Years!

- Downloadable PDFs (www.ecfirst.com):
 - The Disruption of Healthcare
 - Medical Records at Risk!
 - Cyber Security Strategy
- Talk to ecfirst about your compliance & security challenges
 - 1.877.899.9974 x17
 - Lorna.Waggoner@ecfirst.com