IBM Cyber Security Report on the Threat Landscape

- 1,400 is the average # of attacks on a single organization; weekly
- 1.7 is the average # of incidents; weekly
- 2 most common attack forms:
  - Malicious code
  - Sustained probe/scan
- Breaches bottom-line: ~80% human factor based
**HIPAA Final Rule: Key Facts**

- **Key areas impacted include:**
  - Business Associates (BA)
  - Breach Notification
  - HIPAA Privacy Rule
  - Enforcement & Penalties

- **Key Timelines**
  - Final Rule Publication: January 25, 2013
  - Effective Date: This final rule is effective on March 26, 2013
  - Compliance Date: CE/BA must comply by September 23, 2013
  - BAA (Contracts): No later than September 22, 2014

---

**Cyber-attacks: Prepared for Unit 61398 in Shanghai?**

Mandiant, a US-based computer security firm reported on February 19, 2013:

- APT1, a single organization in China focused on cyber espionage, is able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support.

- Traced the hacking activities of APT1 to the site of 12-storey building in the Pudong area of Shanghai
  - It said that Unit 61398 of the People’s Liberation Army "is also located in precisely the same area" and that the actors had similar "missions, capabilities and resources".

- Staffed by hundreds, possibly thousands, of proficient English speakers with advanced computer security and networking skills.

- Hacked into 141 companies across 20 industries, 87% based in English-speaking countries, and is able to steal from dozens of networks simultaneously.

- Stolen hundreds of terabytes of information including blueprints, business plans, pricing documents, user credentials, emails and contact lists.

*Stayed inside hacked networks for an average of 356 days, with the longest lasting 1,764 days.*
Target Breach

- POS malware compromises cash registers that monitor card authorization process
- RAM-scrapping malware steals unencrypted data from memory
- Stolen information copied to a compromised internal system & transmitted outside
- Before a transaction can be authorized, card data is momentarily decrypted & stored in memory (RAM)
- 110 million impacted
- Senior Target executives, including CFO, are witnesses in federal committee hearings

Demand for hackers with POS malware expertise fast rising

Neiman Marcus Breach

The New York Times (Jan 27, 2014)
- Breach was deeper than previously reported
- Hackers invaded systems for several months
- 1.1 million cardholders impacted
- POS malware installed on NM stores appeared to be same malware that infiltrated Target
- NM data stolen from July 16 thru Oct 20, 2013
- NM not aware of breach until mid-Dec 2013

Bottom-line Fact:
50% of Fortune 1000 firms each year experience a breach of 1,000 to 100,000 confidential records, including those of employees
Ponemon Institute (The New York Times, Jan 27, 2014)
Coke Compromised

The New York Times (Jan 27, 2014)

- PII on 70,000 workforce members compromised (including contractors, vendors)
- Data not encrypted stolen by a former worker responsible for maintaining & disposing of company equipment
- Recovered 55 company laptops in Nov/Dec 2013, stolen over 6 years
- Breach discovered Dec 10, 2013
- Senior executive leaves Dec 12, 2013
- Breach disclosed Jan 23, 2014
- Coke assesses over 200,000 files on recovered computers to determine whose PII had been breached
- Stolen computers belonged to employees who worked in HR & had access to HR records

Insider threats must be within scope of risk analysis

Heartbleed Bug Impact on Healthcare

- Hackers exploit Heartbleed bug - U.S. Govt. warns banks, infrastructure operators & others to be on alert for hackers who may steal data from vulnerable networks.
- Heartbleed bug allows hackers to steal data without a trace. Hackers are exploiting bug in OpenSSL code by scanning targeted networks.
- Organizations need to patch & test systems to make sure vulnerability associated with Heartbleed OpenSSL bug is addressed.
- Heartbleed OpenSSL bug vulnerability went undetected for some time. Hackers may have stolen certificates & keys leaving data vulnerable to spying.
- OpenSSL software helps encrypt traffic with certificates & keys that keep information secure. Heartbleed bug exploits OpenSSL vulnerability.
- The developer who reviewed the code failed to notice the Heartbleed bug. Review your patch policy.
## Compliance Fines

### A Seven Figure Risk

<table>
<thead>
<tr>
<th>Date</th>
<th>Entity</th>
<th>Breach Description</th>
<th>Fine</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 7, 2014</td>
<td>Skagit County, Washington</td>
<td>EPHI of 1,581 individuals were accessed by unknown parties after it had been inadvertently moved to a publicly accessible server.</td>
<td>$215,000</td>
</tr>
<tr>
<td>December 20, 2013</td>
<td>Adult &amp; Pediatric Dermatology, P.C., of Concord, Mass., (APDerm)</td>
<td>An unencrypted thumb drive containing EPHI of approximately 2,200 individuals was stolen from a vehicle of a staff member.</td>
<td>$150,000</td>
</tr>
<tr>
<td>August 14, 2013</td>
<td>Affinity Health Plan</td>
<td>Impermissibly disclosed PHI of up to 344,579 individuals when it returned multiple photocopiers to a leasing agent without erasing the data contained on the copier hard drives.</td>
<td>$1,215,780</td>
</tr>
<tr>
<td>July 11, 2013</td>
<td>WellPoint Inc.</td>
<td>Disclosed the EPHI of 612,402 individuals by allowing access of such individuals maintained in the application database.</td>
<td>$1.7 million</td>
</tr>
<tr>
<td>June 13, 2013</td>
<td>Shasta Regional Medical Center (SRMC)</td>
<td>Sent email to workforce about medical records of patients without authorization. Disclosed PHI of a patient to multiple media outlets.</td>
<td>$275,000</td>
</tr>
<tr>
<td>May 21, 2013</td>
<td>Idaho State University</td>
<td>EPHI of approximately 17,500 patients was unsecured for at least 10 months, due to the disabling of firewall protections at servers maintained by ISU.</td>
<td>$400,000</td>
</tr>
<tr>
<td>September 17, 2012</td>
<td>MEEI</td>
<td>Unencrypted personal laptop containing PHI of MEEI patients and research subjects was stolen.</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>June 26, 2012</td>
<td>Alaska DHSS</td>
<td>USB drive containing PHI was stolen from the vehicle of a DHSS employee.</td>
<td>$1.7 million</td>
</tr>
<tr>
<td>March 13, 2012</td>
<td>BCBS T</td>
<td>57 unencrypted computer hard drives containing PHI of over 1 million individuals was stolen.</td>
<td>$1.5 million</td>
</tr>
</tbody>
</table>

### HIPAA Security Rule

- **Device and Media Controls §164.310(d)(1)**
  - **STANDARD**
  - Implement policies & procedures that govern the receipt & removal of hardware & electronic media that contain EPHI into & out of a facility, and the movement of these items within the facility.

- **Encryption and Decryption (A) §164.312(a)(2)(iv)**
  - **Implementation Specification**
  - Implement a mechanism to encrypt & decrypt EPHI.
**HIPAA Security Rule**

- **Transmission Security §164.312(e)(1)**
  
  STANDARD
  
  Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.

- **Encryption (A) §164.312(e)(2) (ii)**
  
  Implementation Specification
  
  Implement a mechanism to encrypt EPHI whenever deemed appropriate.

---

**Massachusetts 201 CMR 17.00**

*Comprehensive Written Information Security Program Required*

- Requires each covered business to “develop, implement, maintain and monitor a comprehensive written information security program” that applies to records that contain Massachusetts’ residents’ personal information
  
  - Security program must include “administrative, technical and physical safeguards” to protect such records
  
  - Designating one or more employees to maintain the comprehensive information security program

- Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information
Massachusetts 201 CMR 17.00

Regulations also require businesses that store or transmit personal information about Massachusetts' residents to (201 CMR 17.04):
- Restrict access by use of passwords
- Deploy updated malware protection
- Encrypt information transmitted across public or wireless networks
- Monitor all systems to detect unauthorized access
- Encrypt information stored on laptops
- Incorporate firewalls

Deadline: March 1, 2010 for 201 CMR 17.00

Massachusetts M.G.L. c. 93H

If an entity knows or has reason to know of either a security breach or that personal information of a Massachusetts resident was acquired or used by an unauthorized person for an unauthorized manner, that entity must provide written notice as soon as practicable and without unreasonable delay to:
- Attorney General (AGO)
- Director of the Office of Consumer Affairs and Business Regulation (OCABR)
- Affected Massachusetts resident

The notice to the Attorney General must include:
- Nature of the breach of security or the unauthorized acquisition or use
- Number of Massachusetts residents affected by such incident at the time of notification, and
- Any steps the person or agency has taken or plans to take relating to the incident
Business Associates

- The changes announced expand many of the privacy & security requirements to BAs that receive PHI, such as contractors and subcontractors.
- BAs may also be liable for the increased penalties for noncompliance based on the level of negligence up to a maximum penalty of $1.5 million.
- The definition of a BA is expanded to include entities or individuals that maintain PHI on behalf of a CE, even if such entities or individuals never access PHI.

A key responsibility of a BA is to ensure it completes a comprehensive risk analysis on a regular, pre-defined schedule.

Breach Notification

- The Final Rule says a risk assessment for determining the probability that PHI was compromised should consider these four factors:
  1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
  2. The unauthorized person who used the PHI or to whom the disclosure was made
  3. Whether the PHI was actually acquired or viewed, and
  4. The extent to which the risk to the PHI has been mitigated

- In the final breach rule, HHS notes: "We have added language to the definition of breach to clarify that an impermissible use or disclosure of PHI is presumed to be a breach unless the CE or BA, as applicable, demonstrates that there is a low probability that the PHI has been compromised."
Results of a Recent HIPAA Audit!

141 High Risk
247 Medium Risk
18 Low Risk
HIGH Probability of Successful Attack

<table>
<thead>
<tr>
<th>THREAT</th>
<th>IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Code Execution</td>
<td>Complete Control of the System</td>
</tr>
<tr>
<td>Unsecured EPHI</td>
<td>Breach</td>
</tr>
<tr>
<td>System configuration issues</td>
<td>Loss of Data</td>
</tr>
<tr>
<td>Buffer Overflow Vulnerability</td>
<td>Denial of Service Attack or Complete Control of the System</td>
</tr>
</tbody>
</table>

HIPAA Checklist!
Establish an Enterprise Program!

The Seven Steps to Enterprise Security™

1. Security Responsibility
2. Risk Analysis
4. Remediate
5. Secure Third Parties
6. Training
7. Evaluate

b i z S H I E L D
### Security Controls Implemented

**What Have You Deployed?**

<table>
<thead>
<tr>
<th>Key Security Controls</th>
<th>Implemented</th>
<th>Missing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall (Sonic Firewall TZ210)</td>
<td></td>
<td>Two-factor authentication</td>
</tr>
<tr>
<td>IDS (Dell SecureWorks)</td>
<td></td>
<td>Data loss prevention solution</td>
</tr>
<tr>
<td>Antivirus protection (Webroot)</td>
<td></td>
<td>Secure text messaging</td>
</tr>
<tr>
<td>Data transfer (SFTP, HTTPS)</td>
<td></td>
<td>USB &amp; portable device encryption</td>
</tr>
<tr>
<td>Remote access (VPN, Citrix)</td>
<td></td>
<td>MDM</td>
</tr>
<tr>
<td>Asset management (Dell KACE)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Laptop encryption (TrueCrypt at the Bios Level; Windows OS &amp; File Vault on Mac OS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email encryption (Voltage)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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 Enterprise Security Program?**

- **Kismet** – A Reactive Security Framework
- **Karma** – A Proactive Security Framework

**China. Target. Coke... Who’s Next?**

WSJ Headline Cover Stories...
Questions?

Are we excited?

For a complimentary HIPAA Checklist PDF please contact John Schelewitz @ +1.480.663.3225 or at John.Schelewitz@ecfirst.com.

From this training, you will learn the following about HIPAA:

- Step through all major sections of HIPAA, HITECH and the Omnibus Final Rule
- Review of the HITECH Act and how it effects all organizations with access to health information
- Examine the HIPAA Privacy and Security Rules; HIPAA Transactions Code Sets and Identifiers
- Review HIPAA compliance challenges; walk through best practices for addressing HIPAA/HITECH mandates
- Step through how to plan and prepare for HIPAA compliance

Denver
May 13-14, 2014

Manila, Philippines
May 20-21, 2014

Chicago
June 17-18, 2014

Washington, D.C.
July 22-23, 2014

Las Vegas
Nov 18-19, 2014
From this compliance and security training program you will:

- Examine HITECH & the HIPAA Security Rule, including new Final Rule updates
- Learn about FISMA, NERC CSS, & GLBA
- Step through the core requirements of PCI DSS.
- Analyse the international security standard, ISO's 27001, ISO 27002, ISO 27799 & others.
- Examine California's SB 1386, SB 541, AB 1950, AB 211 & other U.S. State information security related regulations.
- Understand NIST security standards

Denver
May 15-16, 2014
Manila, Philippines
May 22-23, 2014
Chicago
June 19-20, 2014
Washington, D.C.
July 24-25, 2014
Las Vegas
Nov 20-21, 2014

ecfirst Compliance & Security

Industry leader delivering world-class services in Compliance & Information Security for over a decade

Over 2,100 clients served including Microsoft, Cerner, HP, State of Utah, PNC Bank, Kaiser & hundreds of hospitals, government agencies, business associates

Recognized as an Inc. 500 Business in 1st year of eligibility

Unique, business-driven, compliance and security solutions; based on the proprietary bizSHIELD methodology

Minority Business Enterprise Certified
Ali Pabrai,
MSEE, CISSP (ISSAP, ISSMP)
Follow ecfirst for Daily Tips

Information Security & Compliance Expert
• Consults extensively with technology firms, government agencies and business associates
• Created bizSHIELD™ – an ecfirst Signature Methodology - to address compliance and information security priorities
• Featured speaker at compliance and security conferences worldwide
• Presented at Microsoft, Kaiser, Intuit, E&Y, Federal & State Government agencies & many others
• Established the HIPAA Academy and CSCS Program– gold standard for HIPAA, HITECH compliance solutions
• Member InfraGard (FBI)
• Daily Compliance Tips: www.facebook.com/ecfirst
• Keep in touch, Pabrai@ecfirst.com and www.facebook.com/Pabrai.

Did you get information of value from this brief?
“Like” ecfirst on