STACH&LIU

Pentest Summit 2008
Success Stories and Lessons Learned

Prepared for SANS by
Francis Brown, Director of Assessment

June 2nd & 3rd 2008

STACH&LIU

Successful Pentest

- Demonstrates ROI
- Adds value to business
- Focuses on real world risks
- Enables strategic planning
- ***Aligns with regulatory compliance***

Regulatory trends…

STACH&LIU

Continued increasing of…

- # of federal/state laws
- # of industry regulations
- # of publicly reported breaches
- # of security requirements per regulation
- $ costs per breach/compromised records
- $ penalties/fines for non-compliance

STACH&LIU

Regulatory Alignment

- Justification of costs
- Refinement of scope
- Focus of testing activities
- Report formatting & risk ranking
- Business case for remediation

Example: Cost Justification

STACH&LIU

HIPAA

- Mandatory risk and vulnerability assessments
- Section: § 164.308(a)(1)(ii)(A)
- Requirement: *“Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.”*

PCI DSS

- Mandatory application and network penetration testing
- Requirement #: 11.3
- Requirement: *“Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:*

  11.3.1 Network-layer penetration tests

  11.3.2 Application-layer penetration tests.

Example: Reporting

STACH&LIU

HIPAA

- Vulnerability: Excessive Account Privileges
- Section: § 164.312(a)(1)
- Requirement: *“Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).”*

PCI DSS

- Vulnerability: Default Oracle Account/Passwd
- Requirement #: 2
- Requirement: *“Do not use vendor-supplied defaults for system passwords and other security parameters.”*

Example: How much does it cost?

STACH&LIU

Providence Health System

365,000 Patient Records Stolen

Providence | Health System

Notification to affected = ~$3 million

DOJ Fine = $95,000

Credit Monitoring for 2 years = ~$4 million

Credit restoration services for identity theft victims

Cover all direct financial losses to those affected

Upgrades to information security program

Pending: $1 million suit by terminated employee

DISMISSED: Class action law suit by affected

Northwest Hospital Chain Loses Patient Data

Stolen Laptop Contains Unsecured Data on 365,000 Patients

By Martin H. Bosworth
ConsumerAffairs.Com

February 2, 2006

The latest case of stolen consumer data involves a laptop containing the medical and personal records of 365,000 patients of the Providence Health Care system, which operates hospitals in Oregon and Washington.

The Oregonian • 14-Day Archives | Paid Archives • Subscribe | Today's Paper & More

Ex-worker sues hospital in data loss

Fired - The man alleges he lost his job after reporting that records on Providence patients were stolen from his van

Wednesday, September 05, 2007

ANNE SAKER
The Oregonian Staff

The Providence Health System employee who took home the computerized records of 365,000 patients that were later stolen from his van has sued the hospital, saying he was fired because he reported the theft to authorities.

QUOTE: *"[Providence] will spend **millions of dollars in corrective action** to relieve any harm to affected consumers" -- Attorney General Hardy Myers*

Questions?