Making Better Security Decisions to Reduce Your Business Risks

ISE North America Executive Forum

Bryan Vargo
Sr. Manager, Information Security and Risk Management
McKesson Corporation

November 2011

The latest facts and figures

- **So far in 2011***
  - More than 450 breaches reported
  - Affecting more than 30 million individuals
    - » Retail: 12M+ individuals
    - » Healthcare: 7M+
    - » Government: 4M+
    - » Financial services: 590,000+

- **Loss of reputation and brand value, by the numbers****
  - Average time to restore company reputation after breach: 1 year
  - Average loss in brand value: between 12% – 25%

- **Government clamping down on loss of personal information**
  - Retailers now required to provide customers who have lost PII due to a breach with identify-theft insurance and replacement payment cards (10/27/11)

- **Patients worried sick over U.K. National Health Service breaches**
  - Holding back information and delaying treatment

*Privacy Rights Clearinghouse, Oct 2011
**Ponemon Institute, Oct 2011

Was your data included?

McKESSON
Empowering Healthcare

542,214,872

- Total number of records involved in security breaches containing sensitive, personal information, since January 2005, in the U.S.
- Do you trust that your information assets are secure and accessed properly?
- How big of a threat or breach is needed to get your company's attention?

External Compromises

- **RSA Hack (3/17/2011) :**
  Motive - Unknown attacker, although China believed to be suspect. Motive is probably espionage
  Method - Advanced Persistent Threat (APT) targeted at individuals within an organization using social engineering. Malware hidden in an Excel spreadsheet exploited a zero-day (unpatched) Flash hole.
  Harm - SecurID token deployments at financial, government and other sites were at risk.

- **Sony (Indonesia, Japan , Thailand, Greece , Canada, Netherlands, Europe, Russia, Portugal) & Sony PlayStation Network Hacked (4/6/2011-6/8/2011) :**
  Motive - Lulzsec ,Anonymous, Lebanese hacker Idahc and various other hackers organized the attack in retaliation for Sony attempting to identify visitors to PlayStation 3 hacker George Hotz ' blog site, as well as seeking data from his Twitter and YouTube accounts as part of a lawsuit. The case was later settled out of court.
  Method - Distributed Denial-of-Service (DDoS), SQL injection
  Harm - Defacement of various domains of Sony and Personal information of 77 million people, including customer names, addresses, e-mail addresses, birthdays, PlayStation Network and Qriocity passwords, user names, online handles and possibly credit cards were exposed.

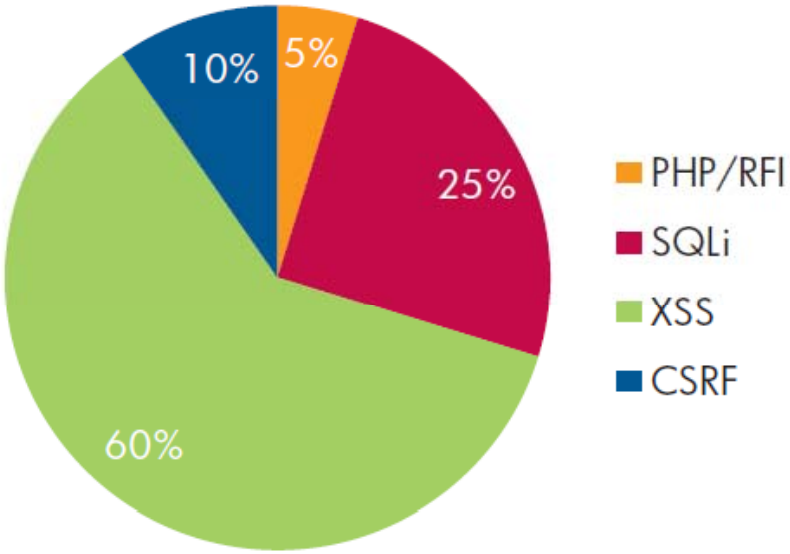
External Healthcare Compromises
Past 6 months

McKESSON
Empowering Healthcare

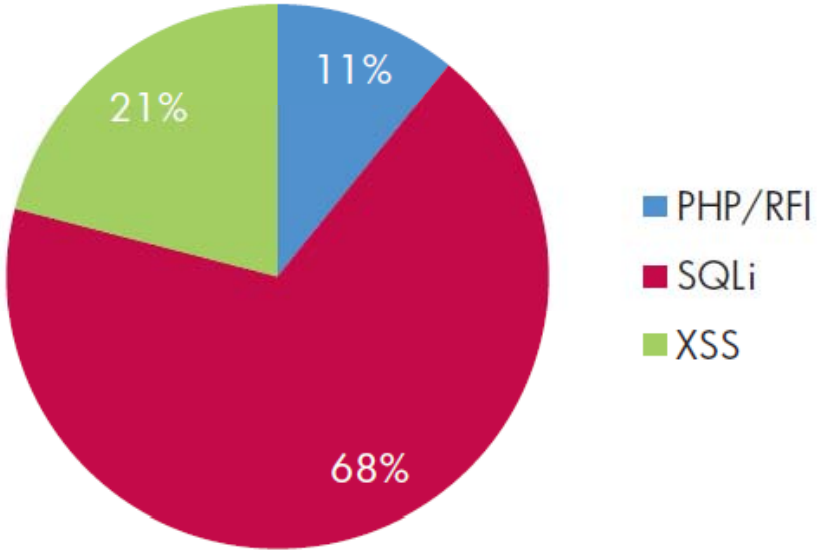
- **3.5K medical records of Genentech; unauthorized person accessed a vendor's computer**
  - http://threatpost.com/en_us/blogs/thousands-patients-risk-id-theft-following-genentech-breach-101311
- **20K patient records of Stanford Hospital; billing contractor posted a spreadsheet on a public forum, asking how to convert it to a bar graph**
  - http://nakedsecurity.sophos.com/2011/09/09/standford-hospital-leaks-20000-patient-records
- **400K medical records from Spartanburg Regional, Unencrypted PC stolen from employee's car**
  - http://news.softpedia.com/news/Stolen-Spartanburg-Regional-Computer-Contains-400k-Patient-Records-212378.shtml
- **4.9 million medical records of TRICARE; missing unencrypted backup tapes**
  - http://threatpost.com/en_us/blogs/49-million-affected-military-healthcare-breach-093011
- **8.6 million records from UK NHS, unencrypted laptop stolen from storage facility**
  - http://threatpost.com/en_us/blogs/laptop-containing-86m-medical-records-lost-uk-061511

SQLi Popularity

SQLi vulnerabilities make up a quarter of the new vulnerabilities reported for the first half of 2011; SQLi attacks make up more than 60 percent of the Web application attacks.



Web application vulnerabilities disclosed, January–June 2011



Total Web application attacks, January–June 2011

- TippingPoint

Impacts to the Business

Threat	Impact
SQLi (Most common)	• Data Extraction • Data Modified • Data Deleted • Full compromise of application data!
XSS	• Fake anti-virus and codecs • Fake flash and Firefox updates • Fake warez and botnet command and controls • Compromise of data
PHP/RFI	• Exploits reputation based Web sites • Compromise of data

Ensure a secure environment

McKESSON
Empowering Healthcare

- As security practitioners we must be as agile as attackers
- Reduce the vulnerability noise by continually testing potential attack paths. Narrow down vulnerabilities and focus on actual risks.
- Establish effective lifecycle principles within your security programs, policies and processes.
- Build metrics that matter not what you can cobble together. Measure effectiveness and make modifications as needed
- Have an accurate inventory of top critical business systems and environments. Know the connected systems and their potential impact to critical business systems.

Ensure a secure environment

(continued)

McKESSON
Empowering Healthcare

- Increase the frequency of your security awareness education. Test your users for susceptibility to phishing and train developers on how to perform secure coding practices.
- Company's and their service provider should be proactive on security programs and remediation efforts. If you wait too long, business impact could occur.
- Get personally involved to show executive level sponsorship of enhancing your company's security posture. Challenge IT resources and security teams to update threats frequently and remediation strategies.

Advantages of Continuous Testing

McKESSON
Empowering Healthcare

Driving better decisions to reduce business risk

A real-world approach to security testing:

- **Simulate and replicate attacks and target your own assets**
- **Pinpoint and prove real risks in your environment**
- **Identify attack paths leading to your critical assets**
- **Convert big data into actionable analytics**
- **Speak in the language of your business, not the whiz kids on your security team**
- **Proactive vs. reactive posture when it comes to security decisions**
- **Efficient, precise and cost-effective remediation priorities = Accurate information and corrective actions with minimum business disruptions**
- **See business information systems and networks through the eyes of attackers to prevent various forms of an breaches**

Benefits for the business

- **Align with corporate goals**
  - Protect brand, reputation and valuation
  - Retain customers and avoid fines / penalties
- **Align with corporate performance objectives**
  - Prevent system downtime
  - Mitigate risks to intellectual property and customer data
- **Comply with mandates for proactive controls assessment**
  - e.g., PCI, FISMA/NIST, HIPAA, SOX, GLBA
- **Increase security efficiency and effectiveness**
  - Automate for increased assessment scope and frequency
  - Reduce consulting expenditures
- **Practice process excellence**
  - Conduct documented, repeatable security tests
  - Validate and verify security using established best practices

Questions and Contact Info.

- Questions?

- Contact Information:

Bryan T. Vargo, CRISC, CCM, CICP
Sr. Manager, Information Security and Risk Management
McKesson Corporation
(608) 348-8087 Direct
(563) 213-0456 Mobile
Bryan.Vargo@McKesson.com
http://www.linkedin.com/in/bryantvargo