



Jacadis, LLC

Securing Web Applications

Ohio WEB Leaders Meeting

May, 29th, 2009

Doug Davidson and Simon Herring

Agenda...

2

- Introduction
- Current Environment
- Securing Web Applications
 - Top-3 Management mistakes
 - Top-3 Technical mistakes
 - Secure Software Process
 - “Security Mix”
- Q & A

Who is Jacadis...

3

- Columbus, Ohio based
- Founded 2001
- Ten staff members with over 17 years on average in Information Security and Technology
- Award Winning Information Security Provider
 - Columbus Technology TopCAT Finalist Outstanding Startup
 - Campus Technology “Innovator 2008 Award” for Best Enterprise Security Project
 - Finalist ComputerWorld Infrastructure Awards – Info security category
 - Featured national speakers, presenters, and subject matter experts



Business & Technical Landscape...

4

- Mobility
- Interconnectedness
- Virtualization
- Cloud Computing / Software as a Service
- Increased Complexity, Volumes of information
- New Technologies (e.g. Web 2.0) increasing collaboration

Web Applications are Vulnerable...

5

- 2007 Acunetix study:
 - “70% of the websites scanned were found to contain high or medium vulnerabilities”
 - “50% of the websites with instances of high vulnerabilities were susceptible to SQL Injection while 42% of these websites were prone to Cross Site Scripting”

- Q1 2009 White Hat Study
 - 82% of websites have had a HIGH, CRITICAL, or URGENT issue
 - 63% of websites currently have a HIGH, CRITICAL, or URGENT issue

Threats are changing...

6

- Economic drivers are creating a “market” for crime
 - ▣ ID Theft fastest growing crime
 - ▣ Cyber extortion a growing threat

- Political environment creating a purpose for crime
 - ▣ “Hacktivism”
 - ▣ Threats to infrastructure

- Threats are changing:
 - ▣ Shift from hobby hackers to organized crime
 - ▣ Available hacking tools keep improving
 - ▣ Increased sophistication of attacks

Reaction to Current Conditions...

7

- Government is reacting to conditions
 - Regulatory drivers (HIPAA, GLBA, SOX, etc.) resulting from government action
- Customers are reacting to conditions
 - Class action suits, contractual (B2B) constructs
- Legal system is reacting to conditions
 - Forcing obligations from contracts, precedent, expectations of due diligence / reasonableness
- Third parties are reacting to conditions
 - Creating contractual obligations similar to government regulations in content and scope
 - Shifting risk
 - Requiring trust, stewardship

Average Data Breach Cost...

8

- \$140 to \$230 per record breached
- Average breach in 2008 = \$6.65M

-- Source: The Ponemon Institute

Doomsday scenarios: businesses close

9

- Doomsday scenarios are real:
 - ▣ Sites marketed through search engines
 - ▣ Sites corrupted without backup forced to close
 - ▣ SaaS businesses serving regulated markets breached that lose investment funding

Only Defense ...

10

Be proactive

Top-3 Management Mistakes...

11

- Expectations
 - ▣ Legal obligations
 - ▣ Policy
- Integrate security later
 - ▣ Acquiesce to the business
 - ▣ Secure “on the fly”
- Not us
 - ▣ “good so far!”
 - ▣ Tick-tock

Top-3 Technical Mistakes...

12

- Not demanding structure, process
 - Security standard (WASC, OWASP...)
 - Reaction
 - Best effort
- Awareness
 - “You can do that? Really?!?”
 - The big picture
- Assumptions
 - Technology will prevent this
 - The security team has this covered

Secure Software Process...

13

- SDLC
 - Consistency, quality, cost effectiveness
- How to execute?
 - Agile / SCRUM
 - Team(s) of 3-7
- What about security?
 - CLASP
 - <http://www.owasp.org>
 - Threat model

The "Security Mix"

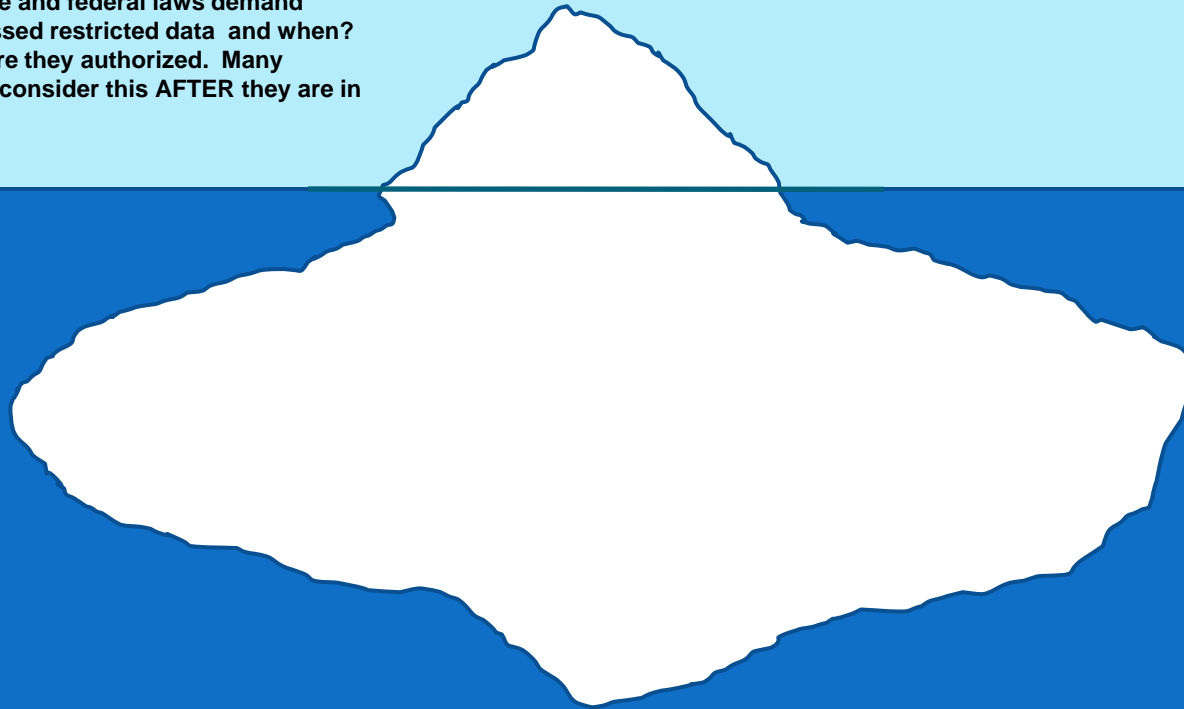
14

- Prevention-Detection-Response
 - Prevent injection flaws
 - Sanitize / validate ALL INPUTS
 - WAF – "virtual patch"
 - Control access
 - Authenticate and Authorize
 - Detect violations
 - Test response capability
- Holistic thinking
 - Systems –vs- Software

Protecting Confidential and Private Data

App vs. Systems approach

HIPAA, SOX, PCI, and state and federal laws demand accountability: Who accessed restricted data and when? How did they do it and were they authorized. Many applications are forced to consider this AFTER they are in production.



Deeper issues

Do you know what CPI collected, where it resides, and how it moves through your organization? Have you communicated confidentiality requirements to employees and stakeholders? Have you limited access by identity and context, secured it where it stored, and ensured that it is handled according to policy and legal requirements? Answering these questions will support compliance... at more than a surface level.

Protecting Confidential and Private Data

App vs. Systems approach

HIPAA, SOX, PCI, and state and federal laws demand accountability: Who accessed restricted data and when? How did they do it and were they authorized. Many applications are forced to consider this AFTER they are in production.



Application

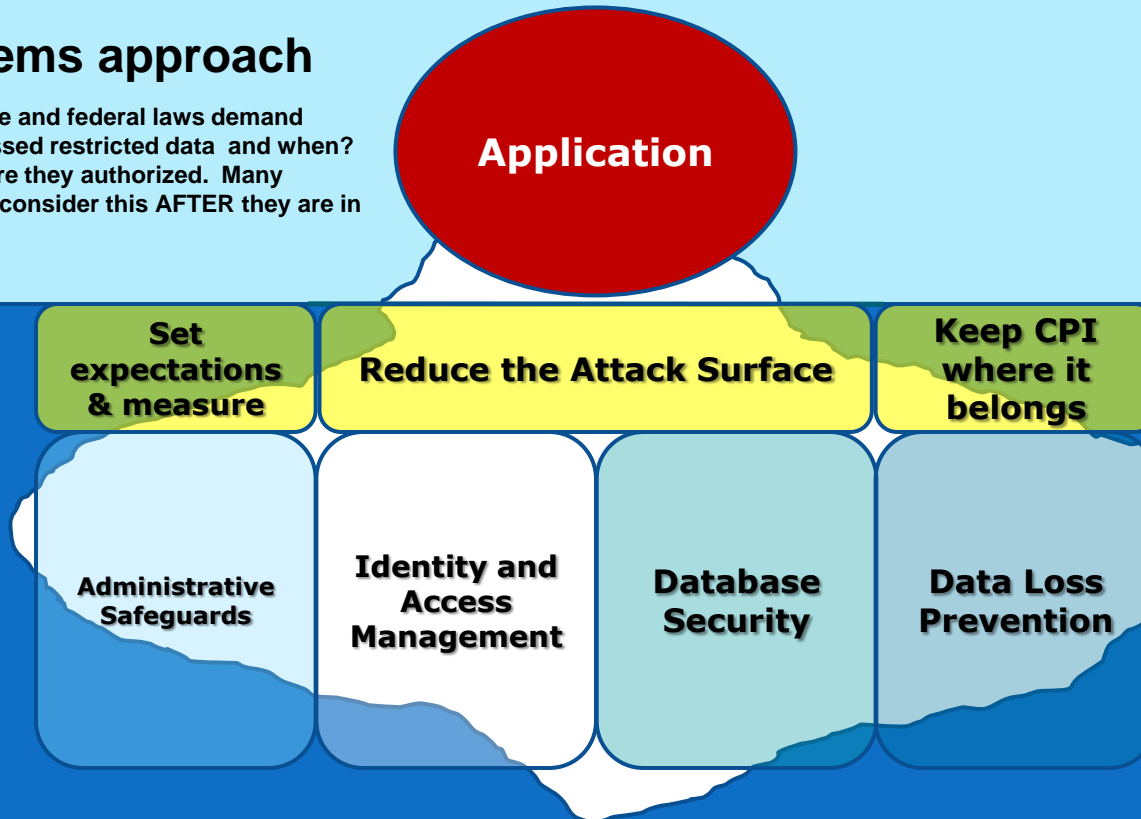
Deeper issues

Do you know what CPI collected, where it resides, and how it moves through your organization? Have you communicated confidentiality requirements to employees and stakeholders? Have you limited access by identity and context, secured it where it stored, and ensured that it is handled according to policy and legal requirements? Answering these questions will support compliance... at more than a surface level.

Protecting Confidential and Private Data

App vs. Systems approach

HIPAA, SOX, PCI, and state and federal laws demand accountability: Who accessed restricted data and when? How did they do it and were they authorized. Many applications are forced to consider this AFTER they are in production.



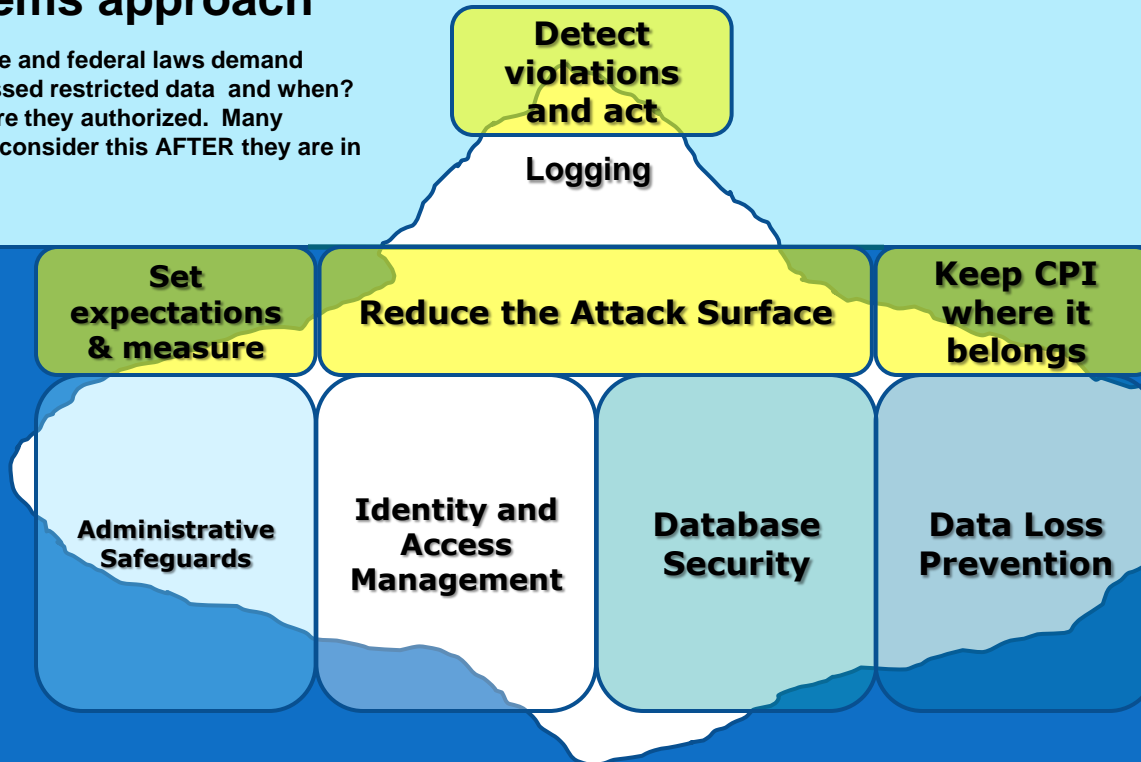
Deeper issues

Do you know what CPI collected, where it resides, and how it moves through your organization? Have you communicated confidentiality requirements to employees and stakeholders? Have you limited access by identity and context, secured it where it stored, and ensured that it is handled according to policy and legal requirements? Answering these questions will support compliance... at more than a surface level.

Protecting Confidential and Private Data

App vs. Systems approach

HIPAA, SOX, PCI, and state and federal laws demand accountability: Who accessed restricted data and when? How did they do it and were they authorized. Many applications are forced to consider this AFTER they are in production.



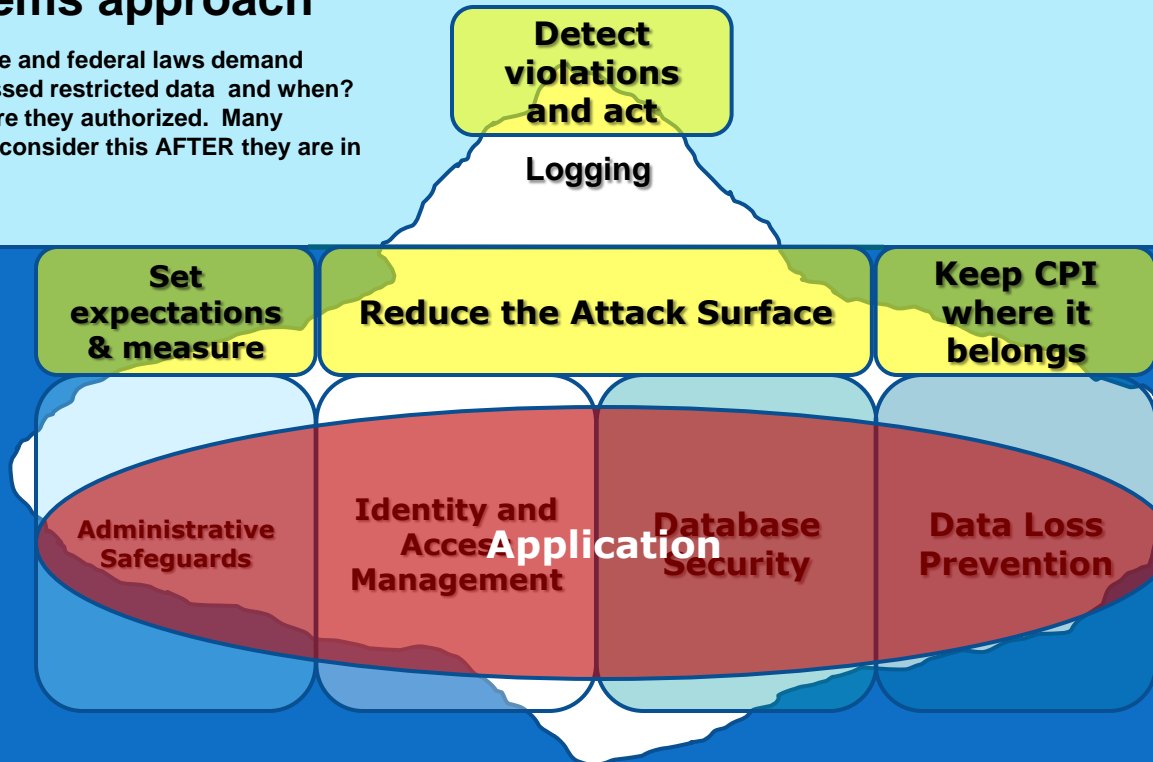
Deeper issues

Do you know what CPI collected, where it resides, and how it moves through your organization? Have you communicated confidentiality requirements to employees and stakeholders? Have you limited access by identity and context, secured it where it stored, and ensured that it is handled according to policy and legal requirements? Answering these questions will support compliance... at more than a surface level.

Protecting Confidential and Private Data

App vs. Systems approach

HIPAA, SOX, PCI, and state and federal laws demand accountability: Who accessed restricted data and when? How did they do it and were they authorized. Many applications are forced to consider this AFTER they are in production.

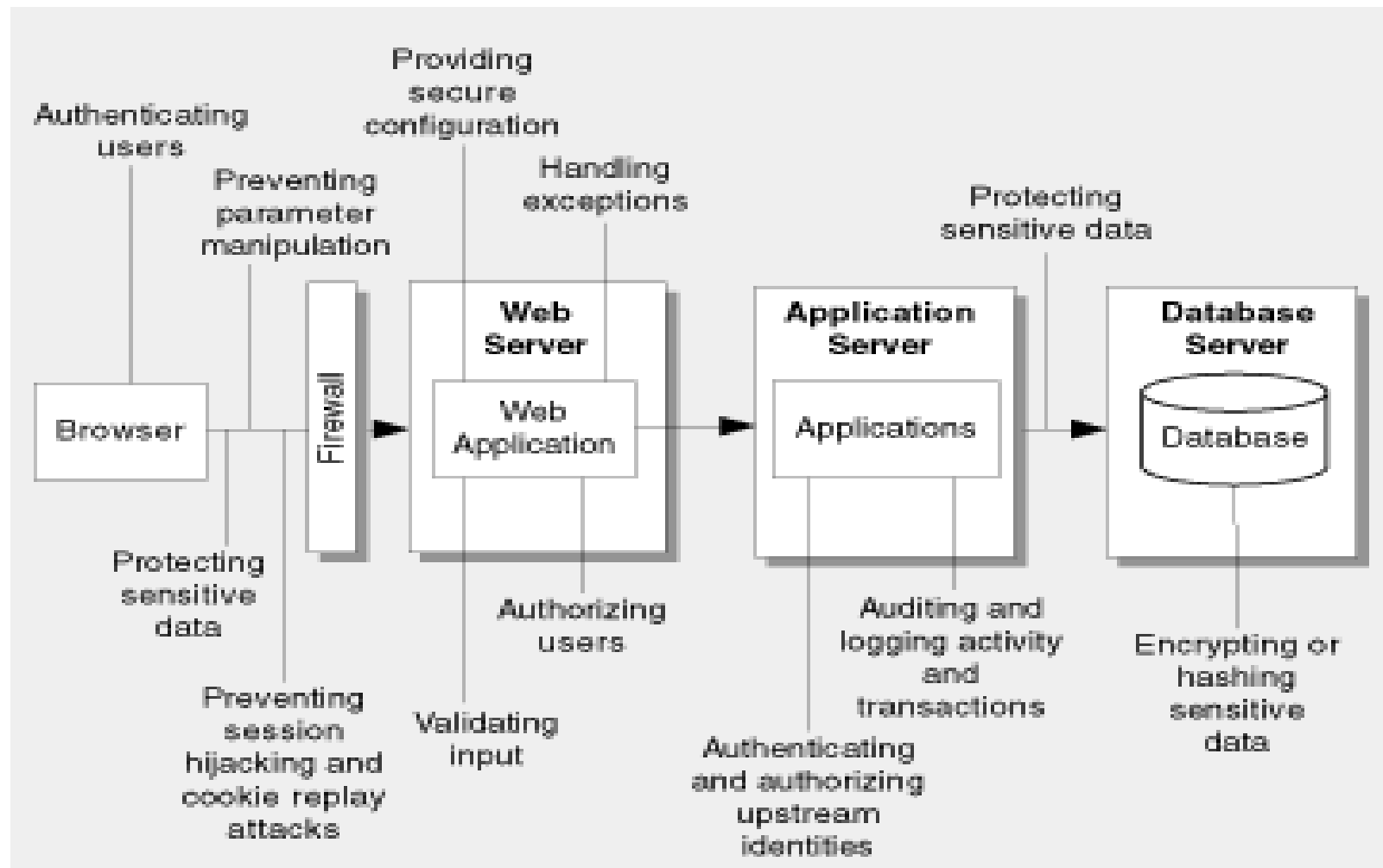


Deeper issues

Do you know what CPI collected, where it resides, and how it moves through your organization? Have you communicated confidentiality requirements to employees and stakeholders? Have you limited access by identity and context, secured it where it stored, and ensured that it is handled according to policy and legal requirements? Answering these questions will support compliance... at more than a surface level.

The Big Picture...

20



Be Proactive...

21

Management

- Know & Own Security Obligations
- Institute security as business requirement
- Risk-based decision making – what could happen to us if ...

Technical

- Demand structure
- Invest in awareness
- Do not rely on technology

Contact Information...

22

Presentation Download

<http://www.jacadis.com/owl.asp>

Doug Davidson

ddavidson@jacadis.com

614-819-0151 x202

Simon Herring

sherring@jacadis.com

614-819-0151 x204

Ask your team ...

23

1. What development methodology do we use?
2. What methodology do we use to identify application threats?
3. Can we prove that we've managed SQL injection and Cross-Site Scripting holes in our websites? Would it take more than 1 day to verify?
4. How do we know who is using our applications? Can we track them from the browser layer to database layer?
5. Would we know it if our website was hacked? Or would we have to wait until a customer, our ISP, or law enforcement notified us?
6. What do you believe your role is in security? Is that sufficient? Do others believe as you do? Is that a good or bad?
7. What behaviors can you change to improve security in your organization? What do you need to start doing that today?