CREATING A SECURE ONLINE PRESENCE

Brandi L. Moore

WHO IS BRANDI MOORE

- Career in Computer Security began in 1997
- AOL Alumni
- Masters in Forensic Science
- Director for Ounce Labs
- OWASP Board Member for NYC Chapter
- Founder of IndiaThink

WHERE ARE WE HEADED?

- Alisa Keimel from Johnny's Seeds (links she mentioned are below)
- http://www.pcicomplianceguide.org
- https://www.pcisecuritystandards.org
- http://www.pcialliance.org

- Risk Management

- Information Security Basics

- PCI Standards

SECURITY IS A PROCESS….NOT A PRODUCT.

Just ask these people….

Firefox File Edit View History Bookmarks Tools Window Help del.icio.us Tue 7:32 PM

A Chronology of Data Breaches

http://www.privacyrights.org/ar/ChronDataBreaches.htm#2008

Getting Started Latest Headlines Gmail: Email from G...

		were in the database could have been compromised.	
July 9, 2008	Wagner Resource Group (McLean, VA)	Sometime late last year, an employee of a McLean investment firm used the online file-sharing network LimeWire. In doing so, he inadvertently opened the private files of his firm to the public. That exposed the names, dates of birth and Social Security numbers of about 2,000 of the firm's clients, including a number of high-powered lawyers and Supreme Court Justice Stephen G. Breyer.	2,000
July 9, 2008	Division of Motor Vehicles Colorado (Colorado)	The DMV regularly sends large batches of personal information over the Internet without encryption and has failed to properly limit access to its database, according to a recent audit. At one point, 33 former DMV employees could access names, addresses, dates of birth and Social Security numbers	3.4 million
July 10, 2008	Williamson County (TN) Schools (Franklin, TN)	Social Security numbers and other personal information of 4,000 children were posted on the Internet.	4,000
July 11, 2008	US Army Fort Lewis (Fort Lewis, WA)	A laptop computer that was reported stolen from an Army employee's truck contained personal information on about 800 to 900 Fort Lewis soldiers. UPDATE (7/11/08) :A 17-year-old Lacey boy faces a charge of suspicion of possession of stolen property after Tumwater police uncovered items from vehicle prowls, including a stolen Army laptop containing information about up to 900 Fort Lewis soldiers.	900
TOTAL number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005.			**233,982,226**

www.PrivacyRights.org

HOME TOP

Copyright © 2005-2008. Privacy Rights Clearinghouse/UCAN. This copyrighted document may be copied and distributed for nonprofit, educational purposes only. For distribution, see our copyright and reprint guidelines. The PRC does not allow any of its documents to be posted on other web sites. The text of this document may not be altered without express authorization of the Privacy Rights Clearinghouse. This document should be used as an information source and not as legal advice. PRC documents contain information about federal laws as well as some California-specific information. Laws in other states may vary. Overall, our information is applicable to consumers nationwide.

Privacy Rights Clearinghouse, 3100 - 5th Ave., Suite B, San Diego, CA 92103. Web: www.privacyrights.org

RISK MANAGEMENT: WHAT'S WHAT

- Risk Management is a technique used by organizations to allocate resources.

- The Process:
  1) Identifying assets
  2) Identifying vulnerabilities
  3) Identifying threats
  4) Evaluating Controls
  5) Determine Risk

WHAT MAKES ME INTERESTING?

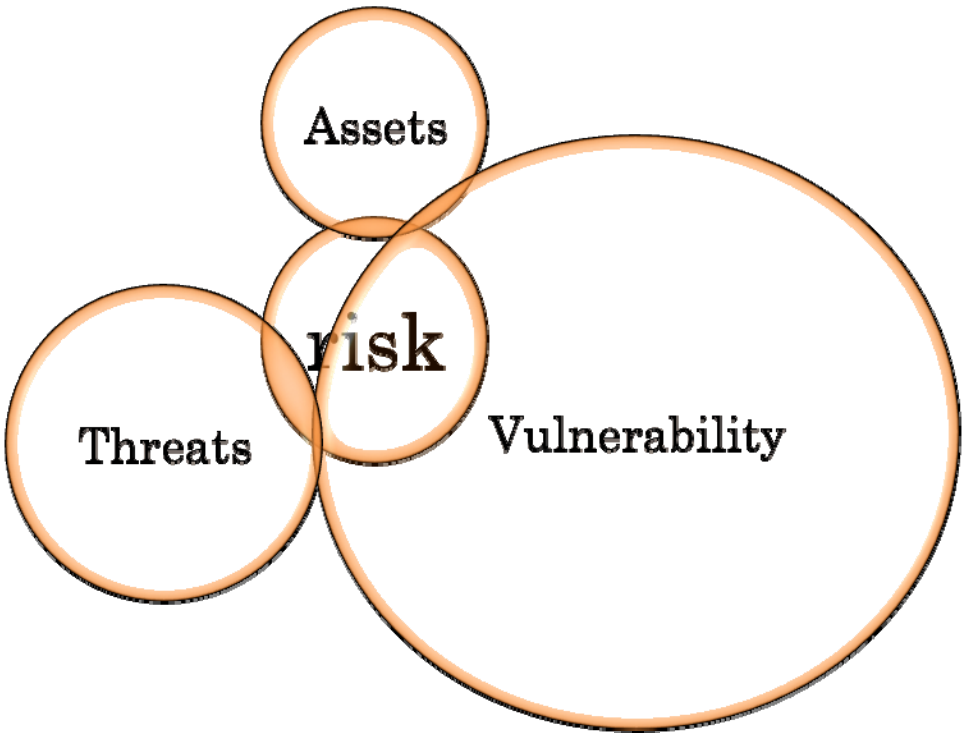
- Customer financial information
- Customer personal information
- Customer transaction history
- Business financials
- Employee Data
- Strategy Documents
- Emergency Response Plans
- Intellectual Property
- Research & Development
- And?

EXAMPLE OF RISK ASSESSMENT

Assets	Vulnerabilities	Threats	Controls	Risk Level
Customer data	theft, destruction, inaccessible	competitors, hackers seeking financial wins, insiders	not encrypting customer data, strong access Control	HIGH
What is valuable to my organization?	How could it be compromised?	Who is interested? Are they skilled?	What are we doing about it?	Assess all answers. Make a risk estimate for priority.

How can I make this asset less valuable to my threats?

RISK EMERGES



LOOK BEFORE YOU LEAP

- Who already has the key?
  - Access Control
  - Interoffice mailings/email
  - Hard documents
  - Public information

Become a control freak.

ONSITE: ACCESSING & STORING INFORMATION

Typical Business Infrastructure contains:

- Servers
  - Access Control
  - Network segmentation (do not face these DIRECTLY to the internet)

- Networking Equipment
  - Router
    - Firewall
    - Do not use defaults
  - Monitor your network
    - "Things seem slow"
  - Wireless Networks
    - Protect with passwords or hide the SSID
    - Do not use defaults

ONSITE: ACCESSING & STORING INFORMATION

- User Machines
  - AV, Spyware, Monitoring Tools
  - Remove Admin control from users
  - Monitor application installs, consider removing ability to install applications.
  - Lock down machines and remove guest users
  - Force users to store information centrally
  - Monitor email usage
  - Is your email hosting provider scanning files?

alesforce.com - Cus... Santa Susanna

	Total Protection™	Security Suite	VirusScan® Plus
Safe Search and Surf Color-coded alerts from McAfee SiteAdvisor to websites to help you avoid online danger.	✓	✓	✓
Always Active, Always Updating Automatically receive the latest software features, threat updates and version upgrades.	✓	✓	✓
Fast Anti-Virus Protection Quickly scans, blocks and cleans out over 200,000 known threats.	✓	✓	✓
Tough Anti-Hacker Protection Hides your online presence and files from hackers, identity thieves and unauthorized communication.	✓	✓	✓
Shrewd Anti-Spyware Protection Intercepts spyware before it installs on your computer and removes existing spyware.	✓	✓	✓
PC Maintenance Cleans clutter off your computer so it stays healthy and secure.	✓	✓	✓
Identity Theft Prevention Guards you from identity theft and online fraud.	✓	✓	
Spam & Online Scam Prevention Shields you from junk email.	✓	✓	
Protects Children Online Blocks offensive websites.	✓	✓	
Automatically Makes Copies Protects your precious online items (files, music, photos) by automatically backing up.	✓	✓	
Home Network Protection Monitors all your home computers and the network if you've linked them together, for security weaknesses and lets you easily share files and printers.	✓		

2007 MONITORING SOFTWARE REPORT

Read the Top Choice Review

Go Right to the Result	Spector Pro BUY NOW ▶	eBlaster BUY NOW ▶	SpyAgent BUY NOW ▶	SpyBuddy BUY NOW ▶	IamBigBrother BUY NOW ▶
RANK	TOP CHOICE	2nd Place	3rd Place	4th Place	5th Place
Features	Spector Pro	eBlaster	SpyAgent	SpyBuddy	IamBigBrother
Overall Features	A	B	B	C	D
Overall Quality	A	A-	B	C	C
Value for the money	A	A-	C	C	C+
Overall Evaluation	★★★★★ Comprehensive recording features, rock solid stealth technology, and excellent customer support. No better value for your money.	★★★★☆ eBlaster is the best remote monitoring software we examined. It sends you detailed reports of everything they do on the PC and Internet.	★★★☆☆ We were impressed with the information that Spy Agent captured, but disappointed when it came time for viewing the log files due to the difficult user interface.	★★☆☆☆ We found SpyBuddy to be full of outdated features and lacking in recording of complete and useful information.	★☆☆☆☆ Not a good value for an inadequate product with a questionable future and poor support.
	BUY NOW ▶ Full Review ▶	BUY NOW ▶ Full Review ▶	BUY NOW ▶ Full Review ▶	BUY NOW ▶ Full Review ▶	BUY NOW ▶ Full Review ▶
RECORDING & LOGGING	Spector Pro	eBlaster	SpyAgent	SpyBuddy	IamBigBrother
Screen Snapshots	EXCELLENT	NO	LIMITED	POOR	LIMITED
Chat / Instant Messages	EXCELLENT	EXCELLENT	GOOD	POOR	LIMITED

OFFSITE: ACCESSING & STORING INFORMATION

- Hosting Provider
  - Start asking questions….they are
    - What security features are part of my contract?
    - How are you going to protect my data?
    - When are they reviewing the security of their datacenter?
    - Who is the group performing the tests?
    - Where can I go for more information?

OFFSITE: ACCESSING & STORING INFORMATION

- Back-up Storage
  - Where are you storing your second copy of data?
  - What are the security policies of the location?
- Outsourcing
  - Application Development
  - Customer Service

PEOPLE: THE WEAKEST LINK

- Awareness Training is the *most effective way* of securing your infrastructure.
- If employees do not open the door, intruders must go to great lengths to enter.
  - Social engineering threats
  - Create good passwords
  - Make employees aware of the value of the company's information

PCI TENANTS

- **Build and Maintain a Secure Network**
  - 1: Install and maintain a firewall configuration to protect cardholder data
  - 2: Do not use vendor-supplied defaults for passwords and other security parameters
- **Protect Cardholder Data**
  - 3: Protect stored cardholder data
  - 4: Encrypt transmission of cardholder data across open, public networks
- **Maintain a Vulnerability Management Program**
  - 5: Use and regularly update anti-virus software
  - 6: Develop / maintain secure systems and applications
- **Implement Strong Access Control Measures**
  - 7: Restrict access to cardholder data by business need-to-know
  - 8: Assign a unique ID to each person with computer access
  - 9: Restrict physical access to cardholder data
- **Regularly Monitor and Test Networks**
  - 10: Track and monitor all access to network resources and cardholder data
  - 11: Regularly test security systems and processes
- **Maintain an Information Security Policy**
  - 12: Maintain a policy that addresses information security

SO WHAT DOES THAT MEAN?

- Steps Small Businesses Need to Follow:
  - Fill out the Self Assessment
  - Work with hosting provider on penetration testing
  - Work with payment processor to insure they are certified and compliant

- What happens if I experience a breach?
  - PCI can increase the overhead you pay on transactions
  - You may be moved to Level 1 where you will be required to perform a full blown audit at a very large expense.
  - PCI may leverage a fine per lost credit card (.05 per card)

SO WHAT DOES THAT MEAN?

- PCI Compliance should be a goal for your organization if you process credit cards.

- The most important thing to remember is that you have help in achieving compliance through your providers BUT you must ensure that the help (payment processor and hosting providers) are doing their part.

- In other words: Don't be the reason for the security breach.

Firefox File Edit View History Bookmarks Tools Window Help del.icio.us Mon 7:36 PM

ASP.NET web Hosting, .NET Hosting, ASP.NET Hosting, Reliable Fast .NET Hosting for Microsoft Developers, ASP Hosting, ASP.NET Hosting, Microsoft Windows 2003 Web Hosting, SQL Server Hosting from EDTHosting.com

http://www.edthosting.com/PCI-Compliant-Hosting.aspx

screen shot on mac

Getting Started Latest Headlines Gmail: Email from G...

empire
DATA TECHNOLOGIES INC.

Home » About Us » Our Data Center » Contact Us » Reseller Hosting » WebMail Login »

Support | Web Hosting | Servers | Domains | My Account

Now Double the Disk Space
Monthly Traffic, and eMail Accounts on all hosting packages!

Toll Free 24x7 Phone Support
1- 877- 455 -7108

www. Search

SHARED HOSTING
VIRTUAL PRIVATE SERVER HOSTING
DEDICATED SERVER HOSTING
SQL SERVER HOSTING
Microsoft FrontPage HOSTING
DOMAIN NAME REGISTRATION
ORDER SSL CERTIFICATES
E COMMERCE SOLUTIONS
PCI Compliant Hosting

EDTHosting.com is a PCI Certified Web Hosting Provider

07-JUL BUSINESS BACKGROUND REVIEWED ControlScan.com
07-JUL VERIFIED SECURE ControlScan.com
ControlScan CERTIFIED

PCI Compliant Web Hosting

PCI Compliant Web Hosting
EDTHosting.com Has Partnered with ControlScan to offer PCI Compliant Web Hosting

Visa, MasterCard, American Express and Discover require all entities that accept credit card payments over the Internet - or process, transmit or store credit card data on a network connected in any way to the Internet - to be certified to meet the Payment Card Industry (PCI) Data Security Standard.

EDTHosting.com has partnered with ControlScan to offer PCI Compliant web hosting to our clients.
All credit card companies and all banks worldwide accept ControlScan's PCI 1-2-3 Certification to validate compliance with the Payment Card Industry Data Security Standards.

To meet these requirements you must complete both the Annual PCI Self-Assessment Questionnaire and pass security scans of your web site(s) and all office, store or other network Internet connection(s) where payment card information is processed or stored. These security scans must be passed on at least a quarterly basis.

There are four steps to becoming "Certified PCI Compliant":

Step 1: Sign up for a web hosting account with EDTHosting.com
Step 2: Completing and passing the annual security self-assessment questionnaire
Step 3: Completing and passing quarterly security scans of your Internet infrastructure
Step 4: Submit your Passed Security Self Assessment & Scan report to your bank.

Step 1: Sign up for a web hosting account with EDTHosting.com

Get started by signing up for a web hosting account with EDTHosting.com. EDTHosting.com is a Certified PCI Compliant web hosting provider. Once you have an account with EDTHosting.com, Log in to your EDTHosting.com control panel account to complete steps 2-4:

Step 2: PCI Compliance security self-assessment questionnaire

When completing the PCI Self-Assessment Questionnaire (SAQ) please keep in mind that it specifically addresses your business practices, computer systems and Web site(s) that are directly involved in processing, storing, or transmitting payment card data.

The PCI Questionnaire will assist you in completing the questionnaire by providing explanations of each question and suggestions for achieving compliance with the requirements.

After completing each section clicking on the "Check Compliance" button at the end of the form will provide a score of the percentage of questions answered and the percentage of passing answers. For your convenience, after clicking the Check Compliance button any questions left unanswered, or indicating an issue needing attention will also be highlighted in yellow. *Click the "Save Changes" button at the bottom of this page at any time to save your work for completion later. If your session times-out while working on the form, please log back in at the login prompt to resume

Step 3: Issuing your ControlScan Certificate of PCI Compliance

Click on Security Scan at the top of this page. Download your passed PCI Scan reports to your desk top. For more information on scheduling PCI Scan please click on the support tab or call ControlScan.

Step 4: Submit your Passed Security Self Assessment & Scan report to your bank.

WHAT'S THE PLAN?

- You figured out what's valuable, set up ways to protect your assets, you met compliance objectives….now what?
  - A computer intrusion can WIPE YOU OUT
  - How will you survive if your database is stolen or destroyed?
  - What happens if your website is down for a week?
  - Business contingency planning is critical to a successful enterprise.
  - Can you afford a large fine from PCI DSS?
  - How will you message your audience about a security problem?
- Act NOW so you don't have to think later.

A Chronology of Data Breaches - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.privacyrights.org/ar/ChronDataBreaches.htm#2008

Getting Started Latest Headlines Salesforce.com - Cus... Santa Susanna

July 14, 2008	Washington Metropolitan Area Transit Authority (Washington, DC)	Metro accidentally published the Social Security numbers of past and present employees on its Web site. The numbers were posted with a solicitation to companies for workers' compensation and risk management services.	4,700
July 15, 2008	Weber Law Firm (Houston, TX)	Sheriff's deputies uncovered hundreds of people's personal financial files that had been discarded in a dumpster in northwest Houston. Box after box of records including personal financial records, documents with Social Security numbers, people's medical files and more were found in the dumpster.	Unknown
July 15, 2008	Missouri National Guard (Jefferson City, MO) (888) 526-6664 ext. 7888 (312) 555-9500 ext. 7888 Soldier deployed overseas	The Missouri National Guard has called for a criminal investigation after it learned that the personal information of as many as 2,000 soldiers had been breached. The Guard would not release how the personal information had been taken -- whether by computer hackers or other means -- because it has asked for a full law enforcement investigation into the matter.	2,000
July 15, 2008	University of Texas at Austin (Austin, TX)	The personal information of University of Texas students and faculty has been exposed on the Internet. An independent watchdog discovered more than five dozen files containing confidential graduate applications, test scores, and Social Security numbers. The	2,500

BrandiLMoore@gmail.com