What's the Hubbub, Bub?
CPOSC
October 16, 2010

INetU Managed Hosting

Introduction

- My goals for this talk:
  - Change of mindset towards compliance and auditing
  - Overview auditing, SAS70, and PCI
  - Open Source tools landscape
  - Lessons Learned

INetU Managed Hosting

About Me

- Wife, Lisa and two children, Riley and Rowan.
- Wrote thesis, “Cash Value Connectivity” that explored the impact of electronic communications on the quality of our lives.
- Recovering Golf-a-holic
- Car Audiophile
- Proposed to my wife in a data center.

INetU Managed Hosting

About Me

- First computer experience on TI-99/4A
- Started an internet business in 1995
- Consulting to internet businesses, Mack Trucks, and Volvo AB
- Open Source Development: larrd for Big Brother
- CISSP, PMP, ITIL, Solaris Admin
- Presently the Director of Client Services for INetU Managed Hosting in Allentown, Pennsylvania

INetU Managed Hosting

Everybody loves compliance and audits!

INetU Managed Hosting

Tabula Rasa

"Blank Slate" – John Locke

INetU Managed Hosting

Trust and Verify

1989: Martin Fleischmann and Stanley Pons

1,064,500

Compliance and auditing is the verification.

Philosophical Sidenote:
“And” and “but” are logically the same: “&”

INetU Managed Hosting

Auditing Basics

- Controls and Control Objectives
- Test Plans
- Evidence
- Populations and samples

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.1 Establish firewall and router configuration standards that include the following:	**1.1** Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:			
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	**1.1.1** Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.			
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks	**1.1.2.a** Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks.			
	1.1.2.b Verify that the diagram is kept current.			
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**1.1.3** Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. Verify that the current network diagram is consistent with the firewall configuration standards.			
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	**1.1.4** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components.			
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure	**1.1.5.a** Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.			
	1.1.5.b Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service. An example of an insecure service, protocol, or port is FTP, which passes user credentials in clear-text.			
1.1.6 Requirement to review firewall and router rule sets at least every six months	**1.1.6.a** Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.			
	1.1.6.b Obtain and examine documentation to verify that the rule sets are reviewed at least every six months.			

INetU Managed Hosting

SAS70

- **Statement on Auditing Standards No. 70**: Service organizations, commonly abbreviated as SAS70, is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). (Wikipedia)
- **Type I** – Auditor's report the service organization has suitable controls implemented in the environment.
- **Type II** – Auditor's report the service organization has suitable controls implemented in the environment **and** the controls were effective during the period under review.

INetU Managed Hosting

SAS70

No standard for exactly what needs to be covered, up to auditor and audited company.

SAS70 reports are generally available upon request (may require NDA).

You want a “non-qualified opinion.”

No fines for “failing.”

INetU Managed Hosting

SAS70

Things that can be covered:

1. Physical Access
2. Environmental Safeguards
3. Network and System Redundancy
4. Network Security
5. Customer Implementation and Maintenance
6. Logical Access
7. Network and Systems Monitoring
8. Problem Management
9. Backup and Recovery

SAS70 Future

It's going away.
SAS70 will be replaced by SSAE 16 starting June 15, 2011.
This is not a major overhaul.

SAS70 to SSAE 16 differences:

Revision control and narratives are required on controls.

"Management assertion" must sign off on accepting the findings of the audit.

An international equivalent is ISAE 3402. This will allow the world to be "on the same page."


POLICE
USMS

INetU Managed Hosting

Working With Auditors

- Don’t lie to your auditors. Take your medicine.
- No findings will make an auditor nervous. Nobody is perfect.
- Auditors don’t have horns, be nice to them!
- Many have this concept called “reasonableness” and “material”
- Haphazard is a real auditor’s method for choosing samples
- Any change to evidence will raise flags with auditors and assessors
- Warn your auditors about changes (very easy to forget)

Deep Thought

Inherent conflict of interests between auditors and clients

INetU Managed Hosting

PCI DSS

- Payment Card Industry Data Security Standards
- Payment Card Industry Security Standards Council 1.0 Released December 15, 2004
- Prevent Credit Card Fraud!
- Applies to all organizations that hold, process, or exchange cardholder information.

INetU Managed Hosting

PCI

- A really bad day (or months)
- T.J. Maxx – 2007 45.6 Million credit card numbers stolen.
- Wireless Woops!
- $5 Million to pay for expenses caused by the breach.
- Albert Gonzales received two concurrent 20-year sentences

PCI

- Annual Assessments
- Internal or External depending on volume of card transactions (Merchants)
  - Level 1 – 6 Million
  - Level 2 – 1 – 6 Million
  - Level 3 – 20,000 – 1 Million e-commerce
  - Level 4 – Fewer than 20,000 e-commerce, up to 1 Million other channels

INetU Managed Hosting

PCI

- Level 1
  - Qualified Security Assessor (QSA) issues Report on Compliance (ROC)
  - Quarterly Network Scan by Approved Scan Vendor (ASV)
  - Attestation of Compliance Form
- Level 2 and 3
  - Annual Self-Assessment Questionnaire (SAQ).
  - Quarterly Network Scan by ASV
  - Attestation of Compliance Form
- Level 4
  - Annual SAQ recommended
  - Quarterly Network Scan by ASV if applicable
  - Compliance validation requirements set by acquirer

PCI 12 Requirements

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.

PCI 12 Requirements

5. Use and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.
7. Restrict Access to cardholder data by business need to know
8. Assign a unique ID to each person with computer access

INetU Managed Hosting

PCI 12 Requirements

9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel.

INetU Managed Hosting

PCI

Not all peachy:

"[PCI DSS] little more than a money-making racket for credit card companies." Dave Hogan CIO US National Retail Federation.

Alternative view:

"If you become secure, compliance comes as a byproduct of security." Bob Russo, General Manager, PCI Security Standards Council

INetU Managed Hosting

“The greatest trick the Devil ever pulled was convincing the world he didn't exist.”

INetU Managed Hosting

Lessons Learned

- Compliance Stick
- Culture of Accountability
- Embrace change management
- Minimize the temptation to change processes as you strive for compliance
- Document how you generate populations and collect evidence.

INetU Managed Hosting

Lessons Learned

The “direction” you audit matters . . . A lot.

Inventory System		Datacenter
SERVER1		FORGOTTODECOM
FATFINGER		SERVER2
SERVER2		SERVER1

INetU Managed Hosting

Lessons Learned

Scope is key.

All changes to production systems must follow the formal change management process.

What do you mean by change?

All firmware upgrades, OS patches, and application code changes to production systems must follow the formal change management process.

Other Compliance Standards

- HIPAA - Health Insurance Portability and Accountability Act – 1996
- SOX – Sarbannes-Oxley Act of 2002
- GLBA – Gramm-Leach-Bliley Act of 1999
- FISMA Federal Information Security Management Act of 2002
- Industry (FDA, SEC, etc.) specific

INetU Managed Hosting

A KISS of Tools

- E-Mail

```
Date: Fri, 15 Oct 2010 16:49:12 -0400 (EDT)
From: scott@loco.packetpushers.com
To: scott@loco.packetpushers.com
Subject: PCI Access Request

Scott,

  Is it OK for John Doe to have access to the production
database servers?

-Scott
```

A KISS of Tools

```
Date: Fri, 15 Oct 2010 16:50:40 -0400 (EDT)
From: scott@loco.packetpushers.com
To: scott@loco.packetpushers.com
Subject: Re: PCI Access Request


Scott,

  Approved.

-Scott

PS - This email may count as evidence for the approval process, but I
don't think it will cut the
separation of duties requirement.  Plus I top replied, but most managers
do that.

On Fri, 15 Oct 2010, scott@loco.packetpushers.com wrote:

> Scott,
>
>  Is it OK for John Doe to have access to the production database
servers?
>
> -Scott
>
```

INetU Managed Hosting

A KISS of Tools

- Cron

```
* */6 * * * root /bin/mail –s “PCI Log Review Reminder” openticket@foo.com < /dev/null

* * */1 * * root /bin/mail –s “PCI Access Review Reminder” openticket@foo.com < /dev/null
```

Ticketing and Request Tracking

- Open Source Trouble Ticket System (OTRS)
  - http://otrs.org/
- Request Tracker (RT)
  - http://bestpractical.com/rt/
- Bugzilla
  - http://www.bugzilla.org/

INetU Managed Hosting

Tools

- Apache mod_security – Core Rule Set
  - Web Application Firewall (WAF)
  - HTTP Protocol validation, bot/crawler detection, SQL injection attack detection, cross site scripting, etc.
  - http://www.modsecurity.org/
- Snare
  - System iNtrusion Analysis & Reporting Environment
  - http://www.intersectalliance.com/projects/Snare/
- Syslog and syslog-ng
- Simple Event Correlator
  - Perl script
  - http://simple-evcorr.sourceforge.net/

INetU Managed Hosting

Tools

- Nessus
  - Network Vulnerability Scanner
  - http://www.nessus.org/
- Nmap
  - Network Scanner
  - http://www.insecure.org/
- Metasplolit
  - Penetration Testing
  - http://www.metasploit.com/
- Nikto
  - Web Server Scanner
  - http://cirt.net/nikto2

INetU Managed Hosting

Tools

- Policy Templates from SANS
  - Because you really want to write policies from scratch, don't you?
  - http://www.sans.org/security-resources/policies/
- Nagios
  - Monitoring, change and problem management and logging
  - http://www.nagios.org/
- Really Awesome New Cisco config Differ (RANCID)
  - Network Device change management
  - http://www.shrubbery.net/rancid/

INetU Managed Hosting

Tools

- Snort
  - Network Intrusion Prevention and Detection System (IDS/IPS)
  - http://www.snort.org/
- OSSEC
  - Open Source Host-Based Intrusion Detection System
  - http://www.ossec.net/
- OWASP
  - Open Web Application Security Project
  - Top Ten: http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Credit where credit is due:
  - http://www.networkworld.com/community/node/60725 - Ben Whaley
  - xforty – Andy Libby, Terry Johnson, Matt Edlefsen

INetU Managed Hosting

Wrapping Up

- Compliance is not inherently evil. Trust and verify is a Good Thing™
- SAS70/SSAE 16/ISAE 3602 – 3rd party confirmation you run a good shop.
- PCI – Reduce credit card fraud.
- Open Source tools can help.
- Compliance is here to stay.

INetU
Managed Hosting

swalters@inetu.net