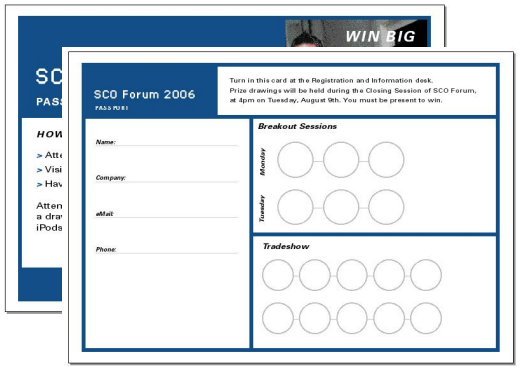
SCO Forum 2006

MOBILITY EVERYWHERE >

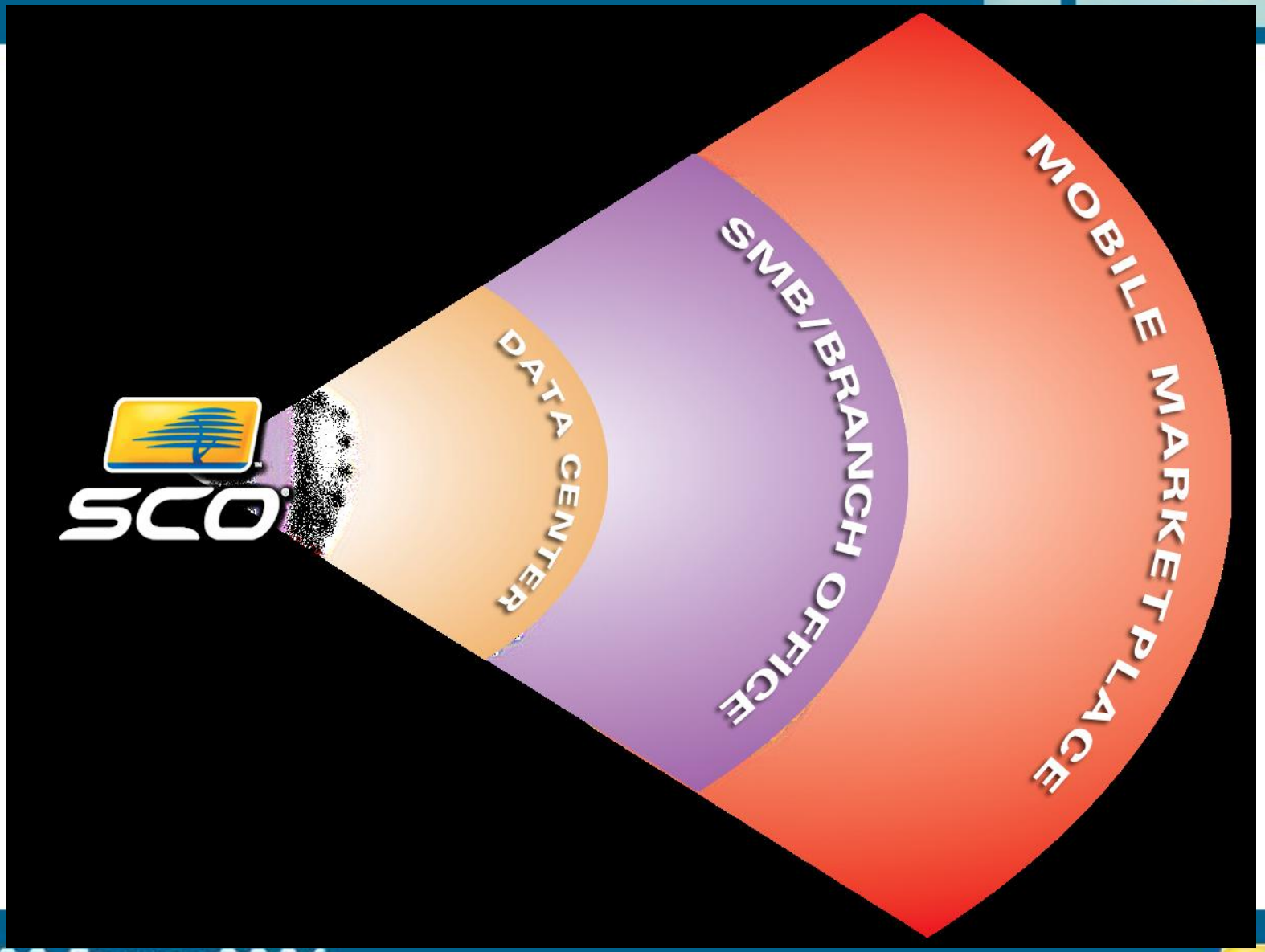
Presentation Title: SOX/PCI Compliance and OSR6 Migration Services
Presenter's Name: Albert Fu
Session ID: 147

Get Your Passport Stamped

- Be sure to get your Passport stamped.
  - Get your passport stamped
    - By breakout session instructor's assistant
    - By exhibitors in the exhibit hall
  - Turn in your Passport
    - After the last breakout session on Wednesday
    - Drawing for great prizes for Wrap-up Session
- Remember to complete the breakout session evaluation form, too



SCO Automates Transactions



SCO UNIX Products

How the topics will be covered

Plan of Attack

- Describe the areas of PS consulting
  - Background on SOX and PCI and how SCO can help
  - Scope of OSR6 Implementation Services
- Focus and clarify by way of example
  - Hypothetical customer who needs assistance in all areas
  - Highlight specific offerings that PS has already completed

Sarbanes-Oxley (SOX) Compliance

How SCO can help you win the battle of Sarbanes-Oxley Section 404 Compliance

Sarbanes-Oxley Legislation

- Enacted into law 07/31/2002
  - http://www.sec.gov/about/laws/soa2002.pdf
- Biggest new regulatory legislation since The New Deal
  - It doesn't just tell you what not to do
  - It tells you *how not to do it*
- Rebuild public trust and prevent future Enrons
  - Everything-but-the-kitchen-sink approach to investor protection
- Biggest UFO your CFO will see
  - Legislation deliberately vague about implementation
  - Competing implementations still require interpretation
  - Scope is large (65 separate sections)
  - Recent SEC estimates place average annual compliance costs at about $25G, or $2M per public company (for large cap companies, >$3M)

SOX Compliance PS Services

SCO can assist *because*

- Auditors cannot also be financial systems providers
- SOX **sec 404** compliance by IT systems substantially falls at the level of OS subsystems
- SOX compliance is good business practice for smaller, private companies

SCO cannot assist with

- One-step SOX compliance software
- Supplying software to manage a SOX Audit
- Performing SOX Audits

SOX Compliance PS Services

Section 404 Compliance Deadlines

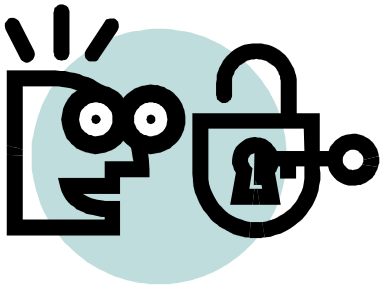
- Most companies: end of FY after July 15, 2007
- Deadline based on market value and report filing history with SEC

Compliance is an annual event

- *You are never done*

Translating Sec. 404 into IT Reality

- Identify all major IT components involved
  - Computer systems
  - Applications
  - Databases
- Choose an Evaluation Framework
  - COSO
  - COBIT
  - COSO + COBIT (http://www.itgi.org)
- Identify Controls and Risks in the following areas:
  - Change Control
  - Access Control
  - Intrusion Detection
  - System Auditing and Logging



SOX Compliance PS Services

Some SCO PS Offerings for Key IT Controls

- Change Control
  - **Patchck** software update and maintenance tool
  - **MIT** and **URK** OS platform replication tool
  - **Porting services** for CVS, RCS, and other source control packages
- Access Control
  - **Centralized Unix user account management** solutions
  - **PAM** (pluggable authentication modules)
  - Customized **ACLs**
  - **Encryption** technology
- Intrusion Detection
  - SCO **File Update Daemon**
  - **Porting services** for Snort, OpenSource Tripwire, AIDE

Some SCO PS Offerings (Continued)

- System Auditing and Logging
  - **EELS + MySQL** + customized scripts
  - Kernel-level **auditing**
  - Opensource **log aggregation tools** (msyslog, syslog-ng)

Payment Card Industry (PCI) Standard

- Established as industry standard in 2004
- All major credit cards used in US, and many world-wide
- Various, similar compliance programs (CISP, AIS, SDP)
- Specifically a data security standard
  - Basically equivalent to applying best practices in IT security
  - 12 requirements in 6 technical areas (network firewalls, encryption, patch and antivirus maintenance, access control, intrusion detection, security policy maintenance)
- Compliance dates/stringency based on Transaction volume
  - Certified audits for large merchants
  - Self-certified Questionnaires for smaller merchants
  - Quarterly network scans for all merchants

PCI Compliance PS Services

Preparing for your PCI Audit or Review

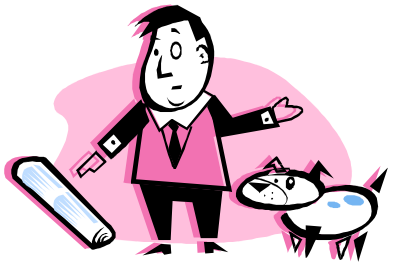
- Read the PCI doc thoroughly
- Read through the Audit and Security Scanning Guides
- Contact SCO for pre-Audit review or customized development
  - Review security scans, remediate, patch
  - Assess security vulnerabilities in OS
  - Bolster access control mechanisms
  - Provide customized logging and intrusion detection systems
- Some pertinent SCO software packages
  - Ipfilter
  - FUD, OpenSource Tripwire, AIDE
  - EELS + MySQL
  - IPSec
  - Patchck

Moving to OpenServer 6 with OSR6 Implementation Services

Related session: 122 (2:30 Tue), 131 (1:30 Wed) “Best Practices in Upgrading to OpenServer 6” by Evan Hunt

What are OSR6 Implementation Services?

- Services are packaged to meet the most common needs
  - Assessment
  - Application Porting
  - Deployment and Replication
  - Training



- Or you can engage SCO Professional Services for
  - Custom-tailored Consulting
  - Custom Engineering

Example: Fictitious Customer + REAL PS Services

Hypothetical Example: WWP
Walking Wrench Plumbing, Inc.

- National Chain of Plumbing and Supply Stores
- Specializing in residential emergency service calls
- Commercial and residential plumbing parts and tools
- 800 stores and service centers nationwide
- Currently running OpenServer 5.0.4 at each location

Example

WWP's IT Situation

- Each store server is P6-class HP/Compaq system running 5.0.4
- Windows-based POS/Kiosks with file sharing via AFPS on SCO
- Parts, inventory, customers managed in SCO Foxbase database
- Serial Printers and Terminals connected via multiport PCI card
- Homegrown daily backup scripting and software
- Brick and Mortar sales transactions on residential service calls
- Network communication to corporate based on telnet/ftp

Example

WWP's Current Limitations and Future Goals

- Customer/Business growth demands more IT processing power
- Consolidation into bigger, centralized super-centers desirable
- Brick and Mortar style of field servicing is slow and inefficient
- FoxBase needs to be migrated
- Serial Printing is a bottleneck under heavy load
- Backup software needs to be migrated
- Network security needs to be improved
- SOX concern with inventory application logging

Example

SCO Assessment of WWP for Migration to OSR6

HARDWARE Assessment

Current HW	Recommendation	Result
Compaq Prosignia 740	Upgrade (SCO-certified)	HP Proliant ML370 G5
64 Mb memory	Increase	4 Gb
Cpqsc SCSI-I, no RAID	Upgrade	HP SAS Drive array in RAID-10 configuration
Laser Printers, serial	Change configuration	IP printers running under CUPS (1.2.2 ported by PS)

Example

SCO Assessment of WWP for Migration to OSR6

APPLICATIONS/SERVICES Assessment

Application/Service	Recommendation	Result on OSR6
AFPS	Config migration	Samba
FoxBase DB	Conversion	MySQL
Business programs	Preserve business logic, modernize	Web-enabled
Backup programs	Port software	Same software

Example

SCO Deployment of WWP OSR6 systems

Task		Result on OSR6
Migrate AFPS		File sharing via Samba
Move user accounts		Identical to 5.0.4
Set up Printers		IP printers under CUPS
Set up storage system		SAS RAID array with SATA backup drive
Check and update security		Latest security patches installed
System Replication		Fast replication via SCO MIT

Example

SCO SOX/PCI Consultation for WWP

Area of Concern	Recommendation	Result on OSR6
Insecure data transfers	Switch to ssh,sftp,rsync	Secure data transfers
Field communications	VPN	IPsec Road Warrior
poor intrusion detection, change control, application logging	SCO custom-engineered FUD + patchck server; EELS/dynamic log import	PCI audit-ready
PCI: Security patch status	Run patchck on server; auto-update clients	Latest patches installed on all systems

Example

SCO Porting of WWP Applications to OSR6

Application	SCO Assistance	Result on OSR6
Openssh, ssl, rsync	Set up, build, test	Packaged deliverables
3rd party business applications	Port to OSR6, add DB interface	Works exactly as in 5.0.4 but with MySQL
Backup scripts	Code review, analyze, modify	Works exactly as in 5.0.4, but enhanced

Example

SCO Training of WWP IT Staff

Area of Learning		Options for OSR6 and other areas
System administration		Written, onsite-delivered
Replication procedure		Included with Deployment Service
OSR5/OSR6 Differences		Written, onsite-delivered
Customized Training (EELS, MySQL, kernel tuning)		Written, onsite-delivered

Example

SCO Custom-Engineered Mobile Field Service Solution for WWP

Area of Concern	Recommendation	Result
Modernize application	Web wrapper or Reimplementation	Java Webservice
Customer data entry	Ericom JavaWrapper or SOAP client	Web/Internet app
Service call processing	Edgeclick ECP connector + Mobile .Net application	Wireless handheld, real-time, GPS
Field POS transaction	Payment processing on Treo 700w + magnetic stripe reader + IR portable printer	Mobile, secure, real-time transactions

Summary

We have seen that SCO PS can

- Help achieve SOX and PCI compliance through the enhancement and addition of OS-level subsystems and applications
- Help create and execute a comprehensive implementation plan for migration to OSR6 (including SOX/PCI concerns)
- Offer a wide range of skills and technologies to achieve any or all of the above
- Integrate an OSR6 server solution with mobile services through EdgeClick

Contact SCO Professional Services

http://www.sco.com/consulting
consulting@sco.com
800-366-8649
ATTN: Yasmin Kureshi
yasmink@sco.com