• The 2008 Chief Information Security Officer (CISO) Agenda
• Goal for the CISO
• Key challenges
  – Regulations
  – Demands from business
  – Approach to Uniform IT Compliance
  – Escalating costs rooted in fragmented approach
  – Access control and identity management
  – Logging and Monitoring
  – Information governance
• Key solutions
  – Protecting intellectual property
  – Organizational realignment
  – Emerging solutions
  – New approaches
  – Security capability model
Risk Management
- New & Emerging Threats
- Compliance Challenges
- Foreign National Threats
- US Federal Government Requirements
- Integration with ERM Initiatives
- Risk Management vs. Risk Elimination
- Evaluation & Prioritization of Risks
- GRC Solutions

Business Enablement
- Changing and Dynamic Business Needs
- Mergers, Globalization, Sourcing
- Customer and Business Self-Service
- Increased Data Portability & Exchange
- Reliance on Third Parties
- Integrity of Key Business Information

Technical Architecture
- Changing view of “perimeters”
- Identity and Access Platforms & Needs
- Security Event Monitoring & Management
- “Data Centric” Security Models & Leakage Protection
- Service Oriented Architectures
- Highly Available Infrastructures
- Security Program Management

Operational Excellence
- Improved Governance Models & Structures
- Improved Budgeting
- Team Structure and Sizing
- Service Level Levels/Management
- Executive Reporting & Metrics
- Managed Security Services
- "How to provide more value with limited resources?"
AL F
He CI
SO-BALANCED
APPROACH

Value Creation Value Creation Value Preservation

- Security as enabler to business needs
- Alignment with business operational benefits
- Solid risk management
- Security as enabler to business needs
- Alignment with business operational benefits
- Solid risk management

- The right control in the right place
- Understanding regulations
- Driving down cost of compliance
- The right control in the right place
- Understanding regulations
- Driving down cost of compliance

Information Protection
Supports
- Better business decisions
- Brand and reputation
- Business initiatives

Business Performance

Risk Management

©2008 KPMG LLP, the US member firm of KPMG International, a Swiss cooperative. All rights reserved. Printed in USA. KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative.
Organizations are struggling with new, updated, and changing regulatory landscape. Some the highlights include:

• Sarbanes Oxley - Section 404
  – AS5 may reduce some burden on IT audit; scope is determined by “risk”
• PCI-DSS – Standards for Credit Card Security
  – Any business who accepts credit card payments are subject to PCI assessments
• Privacy Notification Laws
  – 39+ States have privacy notification laws (including GA, FL, LA, TN, NC); Others have security & Identity Theft laws
  – Potential for Federal Privacy Standards
• NERC – Cyber Security & Reliability Standards (CIP002- CIP009)
  – Increased scrutiny and formalization of penalties (risk & severity)
  – NOPR released in July may have more stringent implications
• HIPAA
  – Healthcare privacy for employees
• FISMA
  – Security requirements for companies or organizations serving US Government
New regulatory pressures and increased business scrutiny is changing the role of the CISO and Security Organizations...

- CISOs are expected to be more business rather than technology oriented
- Operational aspects of security programs are slowly being outsourced or integrated into operational parts of IT
- Security organizations are slowly migrating out of the IT department
- Focus is more of “Risk Management” not “Risk Elimination”
- CISO as an internal advisor rather than manager
- Continued focus on Proactive rather than Reactive approaches
Inconsistent standards and compliance approaches have created inefficiencies including:

- Multiple compliance teams working in silos across the organization
- Process Owners losing productivity due to multiple audit requirements
- More focus on compliance rather than business improvement
- Tactical response to audit findings rather than root cause

Some leading practices have emerged with demonstrable benefits to the compliance efforts:

- Strong focus on Risk Management and assessment of Critical Business Information and Business Processes
- Linking multiple compliance efforts into a more unified approach including consistent governance, planning, and testing
- Leverage well known standards (COBIT, ISO27001, ITIL) to drive organizational improvements rather than silo-ed compliance standards
- Prioritize focus on key areas of compliance focus (Identity Management & Access Control, Change Management, Logging & Monitoring, and Information Governance)
ESCALATING COSTS ROOTED IN FRAGMENTED APPROACH

Is my information current?
What has changed since last time?
What are the right control points?
What are our deficiencies?
Are we fixing our problems?

How effective are my efforts?
Is there an upside to capture?
How much of this can be automated?
Where am I spending my resources?

How can we mitigate the business impact?

Where are we exposed?
What is compliance costing us?

Executives
Managers
Board
Auditor

Internal Controls
SoD
Application Controls
Access Controls
Transaction Monitoring
Control Testing
Documentation
Security Controls
Focus on Access Control and Identity Management will continue to be a priority requirement, consistent across all regulations

- Who is accessing systems and applications?
- What data/information do they have access to?
- Is it appropriate for their job/position?

Some trends include:

- A priority remains the process and technology for provisioning and de-provisioning of users (employees, contractors, customers)
  - Slightly less than previous years
- Focus on Role-Management to identify inconsistencies across the enterprise
- Segregation of Duties analysis is growing concern
- Uniquely identifying “privileged access” users and system accounts
- Regular “certification” of user access
- Improved logging and monitoring of “sensitive” transactions or access
Logging and monitoring requirements are becoming more formalized, with a stronger focus on “proactive” monitoring of logs, looking for potential incidents or issues. This is complicated by:

- Multiple sets of logs (Application, OS, Database, Network)
- Volume of data
- Performance issues

Some trends regarding logging and monitoring include:

- Prioritization of logging and monitoring to critical processes and transactions
- Log standardization including format, configurations, and time synchronization
- Using filters or analytical tools to facilitate “proactive” monitoring
- More intelligent storing and rotation of logs
Information Governance (or Information Management) is an increasing priority for most energy companies. The goal of most Information Governance programs focus on:

- Establishing governance (responsibility, policy, procedures) for organizational Information & Data
- Identifying and prioritizing critical Information Assets
- Developing and Implementing appropriate controls for the Information Assets

Some of the trends in Information Governance we have identified include:

- More focus on Data Classification and Risk Assessments
  - Data ownership is still a tug-of-war between Business and IT
- Increased data portability risks are increasing exponentially
  - Data Leakage tools and processes are starting to mature
- Unstructured data is still a problem for most organizations
- Increased focus on Operational Data rather than just privacy or financial driven information
- Strong linkage to Storage projects and planning
Protecting Intellectual Property

Existing controls may not capture all traffic

< 5%

~100%

Gigabit network pipe

©2008 KPMG LLP, the US member firm of KPMG International, a Swiss cooperative. All rights reserved. Printed in USA. KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative.
CISO / Vice President of Information Security

Security Strategy
1. Investment Prioritization
2. Develop and Maintain Security roadmap
3. Business Liaison (Understand org future needs, align security strategy with business objectives)

IT Risk Management
1. Perform periodic Risk Assessments
2. Measure effectiveness and compliance of accepted standards and governance framework
3. Monitor remediation efforts
4. Audit Liaison

Security Architecture
1. Participate in corporate Architecture Review Board (ARB)
2. Security Tech Review for each initiative
3. Alignment with enterprise architecture, SDLC
4. Provide Security Architectural Support to GIT

Security Services
1. Development & Maintenance of Security Standards
2. Lead Security Solution Implementations
3. Provide Awareness & Training
4. On Demand Services
5. Use of Unlicensed software—Enforce and Attest

Security Operations
** Trending towards reporting up to IT Operations

Threat and Vulnerability Management
1. BCP Testing & Compliance
2. Future Threat Analysis
3. Continually determine security state of GIT
4. Support Incident Response Team/Process
5. Penetration & Vulnerability Testing
6. Malware/Malicious Code Management
7. IP Content Monitoring / Data Loss Prevention

3rd Party Security
1. M&A Due Diligence
2. Vendor Security Program, certification
3. Vendor Security Performance Management
4. Oversee Network Access Agreements (NAA)
<table>
<thead>
<tr>
<th>SC Magazine Award Category</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best Anti-Malware Solution</td>
<td>McAfee VirusScan and Antispyware</td>
</tr>
<tr>
<td>Best audit/vulnerability Solution</td>
<td>Qualys</td>
</tr>
<tr>
<td>Best email Security Solution</td>
<td>Ironport Systems</td>
</tr>
<tr>
<td>Best Enterprise firewall solution</td>
<td>CheckPoint software for Checkpoint VPN-1 Power</td>
</tr>
<tr>
<td>Best Event Management Solution</td>
<td>Trigeo Network Security</td>
</tr>
<tr>
<td>Best Intellectual Property Protection</td>
<td>SecurStar for Drivecrypt Plus Pack</td>
</tr>
<tr>
<td>Best Managed Security Service</td>
<td>SecureWorks</td>
</tr>
<tr>
<td>Best Mobile Device Security Solution</td>
<td>Ironkey</td>
</tr>
<tr>
<td>Best Security Software Development</td>
<td>Fortify Software</td>
</tr>
<tr>
<td>Best Web filtering Solution</td>
<td>WebSense</td>
</tr>
<tr>
<td>Best Wireless Security Solution</td>
<td>AirMagnet</td>
</tr>
<tr>
<td>Best IDS/IPS Solution</td>
<td>TippingPoint</td>
</tr>
</tbody>
</table>

* SC Magazine Awards for 2008 honored in the US on April 8, 2008
In looking at security design, different paradigms that have developed. E-Business is driving security architecture towards a component security framework to accommodate enterprise value-chain integration.

Component Security Framework:
- Component Technology Architecture
- Capabilities Based Organization
- Self-Service and Delegated Administration
- Quality of Service Delivery
- Directory Enabled Security
Information Security Model

**Level 1: Fragmented, Informal & Reactive**
- High level incomplete, weak
- Informal security responsibilities
- No formal staff awareness
- Info Security handled by IT, no one responsible

**Level 2: Fragmented**
- Detailed policies & standards, no endorsement
- Informal security responsibilities
- Alerts & info sent informally
- Reactive, informal

**Level 3: Prevention**
- Formal Risk Assessment, formal responsibilities
- Vulnerability testing, system hardening
- Basic access control, anti-virus on all systems
- Perimeter firewalls, basic AV, ad hoc

**Level 4: Detection**
- Formal Risk Assessment, formal responsibilities
- Some awareness through induction etc.
- Escalation procedures, not always followed
- Vulnerability testing, system hardening

**Level 5: World Class**
- Formally endorsed
- BS7799 accredited, regularly reviewed
- In-depth, redundant, strong, authentication, expert analysis
- 24x7 monitoring, emergency response team
- 24x7 intrusion detection, log analysis

**Security Strategy & Policy**
- Ongoing awareness program & assessment
- Security culture & awareness
- Information Security handled by IT
- No one responsible

**Security Management**
- Dedicated Security Team Board Reporting
- Security architecture & controls
- System hardening, access control
- Perimeter firewalls, basic AV, ad hoc

**Security Culture & Awareness**
- Ongoing awareness program & assessment
- Some awareness through induction etc.
- Escalation procedures, not always followed
- Vulnerability testing, system hardening

**Incident Response**
- Ongoing awareness program & assessment
- Some awareness through induction etc.
- Escalation procedures, not always followed
- Vulnerability testing, system hardening

**Security Architecture & Controls**
- Formally Endorsed
- BS7799 Accredited, Regularly Reviewed
- In-depth, redundant, strong, authentication, expert analysis
- 24x7 monitoring, emergency response team
- 24x7 intrusion detection, log analysis

©2008 KPMG LLP, the US member firm of KPMG International, a Swiss cooperative. All rights reserved. Printed in USA. KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative.
Summary

Most organizations are still struggling with elements of Information Protection driven by emerging and changing compliance and regulatory requirements. The leading companies are creating programs to tackle this at a strategic level.

Leading Practices

Our experience with many in the industry have identified some leading practices that seem to create benefits.

- Create a “unified” approach to various IT compliance initiatives
- Leverage established standards to create a platform for alignment
- No longer a fortress approach to security, data governance is key
- Realign the organization to meet business demands
- Prioritize focus on key security functions to address “root causes” and minimize reactive work:
  - Identity and Access Management
  - Logging & Monitoring
  - Information Governance
Shahed Latif  
Partner  
KPMG LLP, Silicon Valley Office  
slatif@kpmg.com  
(650) 404-4217
Thank You!