



Regulatory Compliance

How to get [and stay] compliant to ANY regulation...

WEI Operations Conference
February 14th, 2007
Newport Beach, CA

Patrick C Miller
CISA CISSP-ISSAP SSCP NSA-IAM SCP TCP

The Current Situation

- Corporate Accountability and Fraud
 - Enron, WorldCom, etc...
 - Id Fraud, Data Breaches, etc...
- Economic Challenges
 - Ripple effect from war(s), oil prices, interest rates, etc; costs are increasing
 - Mandates to do more work with less; budgets are only getting tighter
- Technology Shift
 - Automation is everywhere, doing more work with fewer people
 - Technology gets cheaper by the day, human expertise doesn't
 - Ever-increasing complexity, power and integration/interconnectivity
- Terrorism and Cyber-crime
 - Can they use our people, processes, or technology against us?
 - Organized crime discovered there's good money in hacking
- Lack of Expertise and Experience
 - New talent is scarce; old talent is rapidly exiting the company
 - Security "snake oil" is common; no "easy button"

Regulatory Landscape

Why all the new regulations?

- Aside from the current situation...
- Aside from PDD 67 and HSPD 7...
- Most organizations are **not** implementing good security
- Most organizations do **not** disclose when/how they were hacked (if they know)
- Disagreement on what "good security" actually is or should be
- Unclear or lack of visibility into security within organizations
- Technology has altered the risks; good timing
- Industry self-regulation is getting bad press for moving too slow

When will it get better?

- When we resolve competing security standards that overlap or even conflict
- When Federal agencies producing these regulations can pass their own audits
- It will be a while, so put on your seatbelt and *hang on for the ride...*

NERC is now FERC...

- Energy Policy Act of 2005 created the Electric Reliability Organization (ERO) under FERC
- NERC applied for, and became the ERO
- FERC is reviewing and adopting the NERC Reliability Standards as Federal Law
- So, when all the dust settles...
 - NERC = ERO
 - ERO = FERC
 - NERC Reliability Standards = Law (with penalties that can be up to \$1M per day, per violation)
- Regional Reliability Councils still exist and will perform compliance functions



NERC CIP Standards (001 – 009)

- Critical Infrastructure Protection Standards (CIPS)
- Only 9 of the 130+ Reliability Standards from NERC (ERO)
- Slightly different than other Reliability Standards..
- Implementation plan is specific to type of entity
- Overall, must be compliant by the end of Q2, 2009
- Sanctions and penalties can be levied
- Significant impact to all levels of the business

CIP-001 through CIP-009

- 
- CIP-001 – Sabotage Reporting
 - CIP-002 – Critical Cyber Asset Identification
 - CIP-003 – Security Management Controls
 - CIP-004 – Personnel & Training
 - CIP-005 – Electronic Security Perimeter(s)
 - CIP-006 – Physical Security of Critical Cyber Assets
 - CIP-007 – Systems Security Management
 - CIP-008 – Incident Reporting and Response Planning
 - CIP-009 – Recovery Plans for Critical Cyber Assets

We Are Not Alone...

- 
- CIPS
 - Sarbanes-Oxley
 - HIPAA
 - GLBA
 - CJIS
 - California SB1386
 - AGA-12
 - PCI
 - MTSA (ISPS)
 - SAFETY Act
 - FIPS/FISMA
 - 6 CFR Part 27


Just to name a few...

Common Threads

They all have very similar roots...

- Driven by PDD 67 and HSPD 7
- Built on-or-from ISO 17799/27001
- Risk-based assessments are always Step #1
- Definitely not perfect in current implementations, but the advice is still sound
- None of this is new – based on time-tested general security principles that work for both physical and information assets

General Security Principles

- 
- Defense in depth
 - Least privilege; need to know
 - Separation of duties
 - Keep it simple; complexity increases risk
 - Keep it separate
 - Create distinct zones or segments
 - Firewall example - physical/cyber
 - Be practical
 - Don't over-secure (you don't have to outrun the bear)
 - Remember the 80/20 rule; security is an asymptotic curve

Secret Solution

What is the secret to perpetual compliance?

BUILT-IN SECURITY!

- Be proactive -- not reactive...
- Don't wait for onerous regulations to begin securing your organization or you will always be catching up
- Security must be built into business processes
- Requisite culture-shift (toward security and auditability)
- Build a framework for compliance to **any regulation**

The Right Thing To Do...


Reliability

Compliance

Security



Security vs. Reliability

- 
- Security does not trump reliability
 - Done right, security supports reliability
 - You can be secure and reliable, it is not a myth
 - IT has already invented the wheel, use theirs...
["Visible-Ops" is a perfect example]

The Real Story...

Compliance isn't easy...

- Get organized
- Get ownership
- Get educated
- Get help
- Understanding risk
- Managing expectations
- Sustaining compliance





Get Ownership

- Start with the "tone at the top"
- Letter of the law, or spirit of the law?
- Establish upstream awareness and acknowledgement at every level to provide appropriate assurance
- Establish necessary maintenance requirements -- *maintaining/sustaining compliance is the hardest part*
- Regular audits (internal and external) to ensure that compliance activities are fully "operationalized."

Get Organized

- Identify Stakeholders; have them provide a team of Subject Matter Experts (SMEs)
- Create standard document templates for everything; maintain consistency in the formatting/presentation of the data
- Document your compliance program approach; even something as simple as a project plan will work
- Identify your criticality criteria and risk-assessment method
- Schedule regular self-assessment and self-audits; report all findings to Stakeholders as early as possible
- Dashboards and stoplights are a great ideas and can offer a daily view into the "compliance posture" (works better with good automation); some vendor tools are emerging

Get Educated



- Read other standards from other industries; remember the Energy Industry is not alone
- Review any/all applicable Risk Assessment Methods
- Review the history of your particular regulation/standard to obtain a better idea of where it is going in the future
- Seek to understand how you will be held accountable; become comfortable with the audit process
- Get involved with industry Working Groups and discuss how peers are evaluating and mitigating their risks

Get Help



- More involvement from all areas of the business means less burden on any one particular group
- If the entire business is involved, it will usually take less time and achieve a greater breadth of coverage
- Leverage your IT department expertise with auditable processes; IT already knows how to live within the confines of SOX, CobiT, COSO, ITIL, ITSM, etc...
- Leverage your project management office
- Piggyback on successful operational functions and programs such as Safety

Understanding Risk

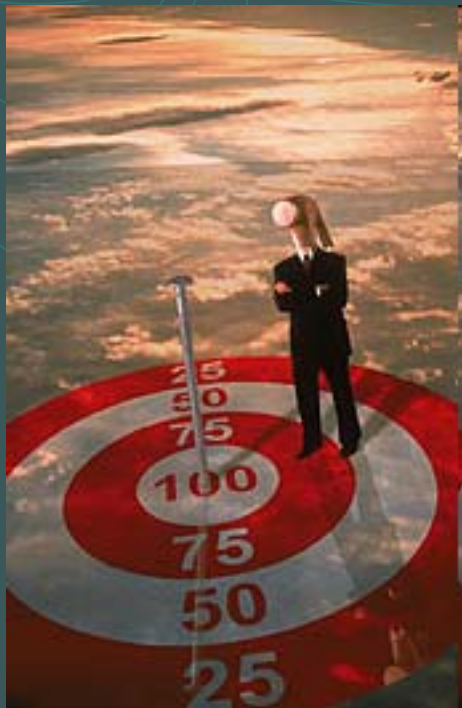
- Risk = Impact x Probability (or in other terms, Consequence x Likelihood) – it's a very simple equation. *Keep it that way.*
- Overanalyzing risk can waste time and money; often the qualitative complex risk assessment methods obtain the same result as qualitative simple methods
- Don't assume risk on your own. Make it a business decision based on good solid facts -- *remember: Management owns the risk.*
- Understand controls, threats, vulnerabilities, exploits, opportunity and how they relate to risk
- The more you know about risk *and* risk assessment the better you will be able to articulate [defend] your position to an auditor



Risk Assessment Resources

- There is no silver-bullet or easy-button tool, and there won't be – *despite what Vendors say*
- In NERC's own words, there are three important questions:
 - What is critical?
 - What is vulnerable?
 - What can be done to reduce the vulnerabilities?
- NERC RAWG Whitepaper
 - <http://www.esisac.com/library-assessments.htm>
- ESISAC – Vulnerability and Risk Assessment
 - <http://www.esisac.com/publicdocs/Guides/V1-VulnerabilityAssessment.pdf>
- NIST 800 series
 - <http://www.csrc.nist.gov/publications/nistpubs/>
- ASIS Guideline
 - <http://www.asisonline.org/guidelines/guidelinesgsra.pdf>
- OCTAVE
 - <http://www.cert.org/octave/>
- Sandia Labs Risk Assessment Classification Scheme
 - http://www.sandia.gov/iorta/docs/SAND2004_4233.pdf
- GAO – Risk Assessment Practices of Leading Organizations
 - <http://www.gao.gov/special.pubs/ai00033.pdf>

Managing Expectations



- Compliance will require a culture-shift; don't try to change too much at once
- Start with a gap analysis to understand just how much work is in front of your compliance team; consider using Maturity Metrics (ISO21827, CobiT)
- Be as clear as possible as on what is necessary to be done, in terms of labor, budget and time
- Regular, **unvarnished** upstream reporting is vital; keep the chain of command informed of everything related to the compliance effort
- Don't rely on FUD (Fear, Uncertainty and Doubt); keep it real, and keep politics out of the discussion
- It may require an occasional reminder that "doing the right thing" is in the organization's best interest

Sustaining Compliance

- Compliance evidence does not need to be complex. Matter of fact, the simpler the better.
- Have the SMEs or the operational staff develop the processes, procedures and other required documentation for a higher degree of ownership and acceptance within the business
- Get it “operationalized” early and hold people accountable with applicable reporting metrics
- Automate, automate, automate; avoid manual processes whenever possible; include logical checks to ensure automation is functioning as expected
- Get compliance language into your RFPs and contracts; e.g. leverage the SCADA Procurement Language project
- Audit yourself regularly; use appropriate internal *and* external resources

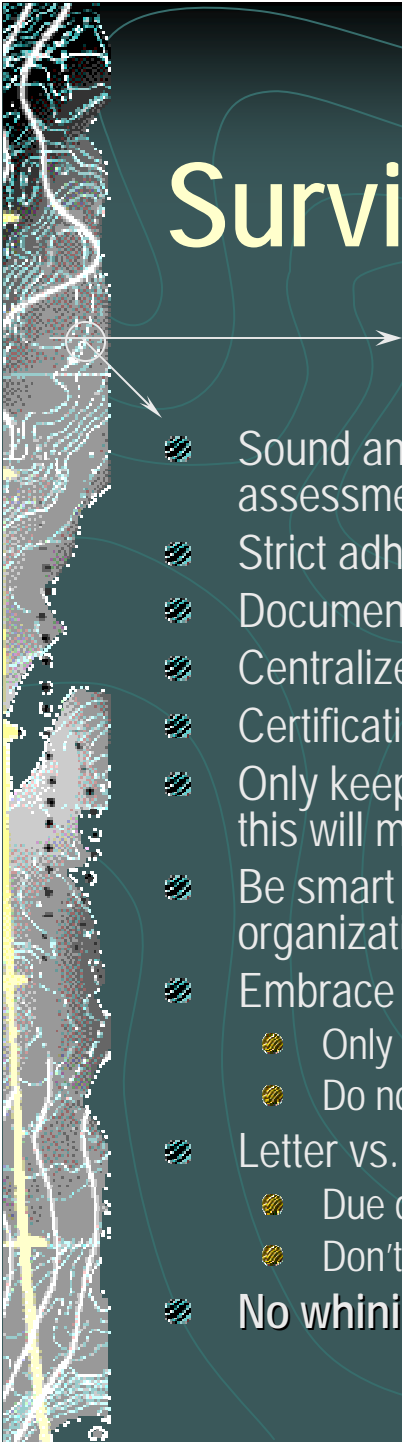
Program Elements That Work

- Design a program architecture that spans entire organization
 - Senior Management sponsor – signing Officer, directs program, accepts risks
 - Stakeholders – Directors [and above] with skin in the game
 - Subject Matter Experts – Ops staff; where the rubber hits the road
- Document all known gaps, even the bad stuff; assign [realistic] owners and dates to all issues and hold them to it – drive it like a project
- Capture all decisions, discussions and meetings for the audit record
- Compliance summary for management; stoplight or dashboard
- Formal process for exceptions/deviations; include standard risk language
- Strong chain of accountability; require upstream signatures
- Use of logs, audit trails, and any other technical means to establish all necessary evidence; less reliance on human processes where appropriate
- Storage of all documentation and evidence in a tightly controlled central repository; “evidence catalog”
- Checklists for regular self-assessments/self-audits

What About the Money?

- Do you spend more on coffee or A/C than security?
- Many PUCs/PSCs have openly stated you'll get the money needed to be secure (and compliant)
- Good protection isn't cheap, so spend wisely
- In-house vs. out-sourcing – depends on size
- Don't forget about cost-avoidance; is doing the work upfront cheaper than fines, auditors and lawyers?
- Consider the automobile safety push in the 1970s – Volvo and Subaru capitalized on it
- Be the most secure and reliable company on the block – it's all we've got!

Surviving an Audit

- 
- Sound and comprehensive risk assessment as your baseline; regularly repeat the assessment using the same criteria for consistency
 - Strict adherence to your [self-defined] policy, processes and procedures
 - Document everything; meeting minutes, decisions, discussions, exceptions...
 - Centralized location and format for all compliance documentation
 - Certification and signatures all the way upstream, starting with the SME-level
 - Only keep/provide what is required as evidence for compliance; don't over-provide – this will minimize drill-down and diversions
 - Be smart and confident in your compliance efforts, only you know what is best for your organization; respectfully challenge the auditor if necessary
 - Embrace ambiguity in your responses to auditors
 - Only tell them exactly what they need to know, with only as much detail as necessary
 - Do not volunteer anything beyond what is explicitly asked
 - Letter vs. spirit of the law
 - Due diligence and due care – both are required
 - Don't rely on an auditor's interpretation; compliance should be immediately apparent
 - **No whining**; take your licks like a pro (should you get any)

Closing Thoughts...

- You are part of the *Critical Infrastructure* – **act accordingly and responsibly**
- Whether it's corporate accountability or infrastructure security, the laws are changing and you will be forced to change in response
- Build security and accountability into your everyday processes and compliance will follow
- Build a compliance program to meet any new regulation that may come your way, because it will
- *The auditors and lawyers are coming...*

Questions?

Patrick C. Miller

CISA CISSP-ISSAP SSCP NSA-IAM

Sr. Security Consultant

PacifiCorp Corporate Security

patrick.miller@pacificorp.com

503.813.7014