

Information Security for Utility Managers

Patrick C Miller, CISSP-ISSAP SSCP NSA IAM
Stacy J Bresler, CISSP CISA

November 17th 2005
World Trade Center 2, Portland, OR



Utility Management Certificate
Atkinson Graduate School of Management



Outline

- What is Information Security?
- General Security Principles
- Understanding risks
- Regulations and compliance
- Security organization
- Security spending
- Putting it all together



What is Information Security?

- Past
 - Centered mostly on physical access and secrets
 - A very, *very* old story
- Present
 - Logical access and secrets – serious encryption
 - Hackers, crackers and phishers
 - There's good money in cyber-crime
 - My bot-net can beat up your bot-net
 - Zero-Days and singularities
- Future
 - Cyber-warfare and organized cyber-crime
 - The auditors and lawyers are coming...



Two Sides - Operations & IT

- Operations is no longer separate
- Cultural differences are deep
- Communication and education
- Flexibility is required
 - Technology, procedures, policy, etc...
 - It's all IT, but...
- Same security principles apply*



General Security Principles

- Defense in depth
- Least privilege
- Separation of duties
- Segregation of networks
- Need to know/have
- Keep it simple
 - Complexity increases risk and decreases security
- Be practical
 - Don't over-secure (outrun the bear)
 - Remember the 80/20 rule
 - Know your risk tolerance



Understanding Risk

□ What is Risk?

■ Risk = Likelihood x Impact

■ ...where Likelihood is:

□ Vulnerability – *susceptibility to theft*

□ Opportunity – *lack of access controls*

□ Threat – *potential act of malice*

(Vulnerability x Opportunity x Threat) x Impact



Utility Management Certificate
Atkinson Graduate School of Management



Simplified Risk Example...

An unpatched stand alone PC containing top secret information in a locked room with 24x7 armed guard, cameras and multiple biometric locks -- and only one person is allowed...

Risk = threat x vulnerability x opportunity x impact

Risk = 3 x 3 x 0 x 3

Risk = 0



Utility Management Certificate
Atkinson Graduate School of Management



Measuring Risk

- Qualitative
 - Less expensive, less refined
 - Rough measurements in terms
- Quantitative
 - More expensive, more refined
 - Exact measurements in numbers
- Risk assessments
 - Watch out for FOIA (protect the findings)
 - Choose the right company
 - Annual assessments, at least



Risk Options

Accept

- Do nothing, ignore it, take the hit, etc...
- Free, *at first*...

Mitigate

- Establish controls to effectively work toward reduction of the risk over time
- Can be very expensive

Transfer

- Make it someone else's problem, usually through legal or contractual means



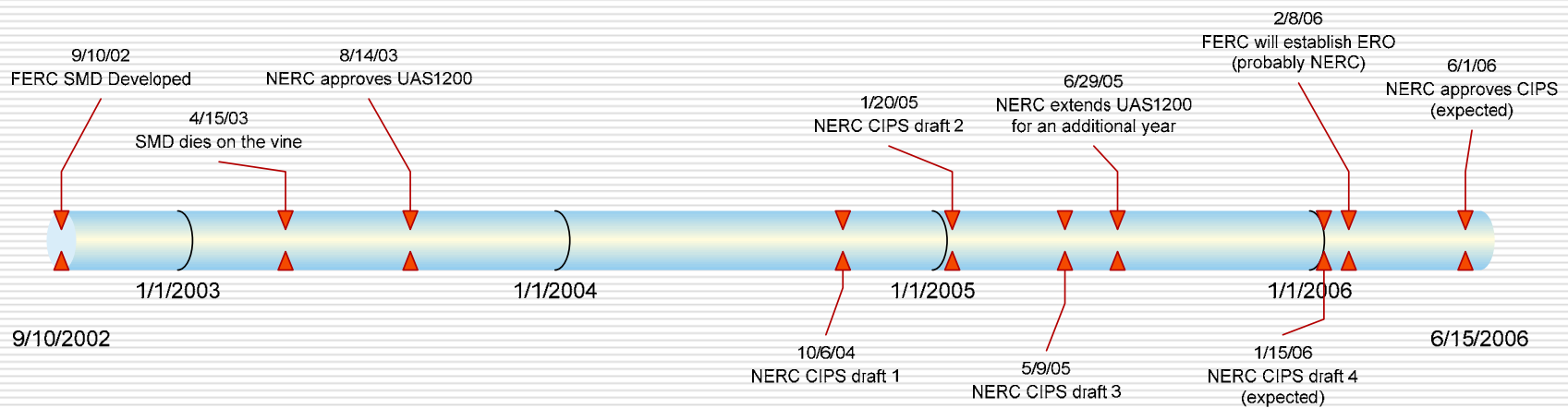
Security Regulations Overview

Get ready for a lesson in acronyms...

- FERC
 - Nothing yet, but what is the ERO?
- NERC
 - UAS1200
 - CIP-002 through CIP-009 (aka, CIPS)
- WECC
 - Guidelines, not standards
- The Department of Homeland Security (DHS) is just getting warmed up...



Regulatory Timeline...



Utility Management Certificate
Atkinson Graduate School of Management



FERC vs. NERC

- FERC (Federal Energy Regulatory Commission)
 - US Government entity
 - Part of the Department of Energy (DOE)
 - Makes laws; has “teeth”

- NERC (North-American Electric Reliability Council)
 - International entity
 - Standards organization
 - Regional councils have “teeth”



FERC: the SMD and the ERO

- ❑ Old: Standard Market Design (SMD)
 - Security tacked onto the end of market design
 - Appendix G was thin, but a great start
 - Died on the vine, so security problem was handed off to NERC for implementation
- ❑ New: Electric Reliability Organization (ERO)
 - Created by the Energy Policy Act of 2005
 - Will *probably* be NERC
 - ERO has “teeth”
 - New NOPRs will be coming



NERC: UAS1200

Urgent Action Cyber Security Standard 1200

- ❑ NERC's version of the FERC SMD
- ❑ Temporary standard, 2 year lifespan
- ❑ Permanent standard (CIPS) delayed, so UAS1200 was extended 1 year
- ❑ Only Control Centers are in scope



Utility Management Certificate
Atkinson Graduate School of Management



NERC: UAS1200

Components of the Urgent Action Cyber Security Standard 1200...

- 1201 – Cyber Security Policy
- 1202 – Critical Cyber Assets
- 1203 – Electronic Security Perimeter
- 1204 – Electronic Access Controls
- 1205 – Physical Security Perimeter
- 1206 – Physical Access Controls
- 1207 – Personnel
- 1208 – Monitoring Physical Access
- 1209 – Monitoring Electronic Access
- 1210 – Information Protection
- 1211 – Training
- 1212 – Systems Management
- 1213 – Test Procedures
- 1214 – Electronic Incident Response Actions
- 1215 – Physical Incident Response Actions
- 1216 – Recovery Plans



Utility Management Certificate
Atkinson Graduate School of Management



NERC: CIP 002-009 (CIPS)

Critical Infrastructure Protection Standards CIP-002 through CIP-009

- Permanent security standard
- Will be adopted by FERC if NERC becomes ERO
- Now in-scope:
 - Generation
 - Transmission
 - Process Control Systems
- Should be adopted by mid-summer 2006
- Self-certify compliance annually
- Audits are every 3 years



Utility Management Certificate
Atkinson Graduate School of Management



NERC: CIP 002-009 (CIPS)

Critical Infrastructure Protection Standards...

- CIP-002 – Critical Cyber Assets
- CIP-003 – Security Management Controls
- CIP-004 – Personnel and Training
- CIP-005 – Electronic Security
- CIP-006 – Physical Security
- CIP-007 – Systems Security Management
- CIP-008 – Incident Reporting and Response Planning
- CIP-009 – Recovery Plans for Critical Cyber Assets

- What is CIP-001?
 - Sabotage Reporting (still in pre-draft)



WECC: Security Guidelines

- Western Electricity Coordinating Council
- NERC Regional Reliability Council for Western US, Canada and Mexico
- Guidelines, not Standards
 - Minimum Physical Security
 - Minimum Physical Security for Control Centers
 - WECC Operations Network (WON)
- Can still impose fines and sanctions



Department of Homeland Security

- ❑ DHS is gaining strength and power
- ❑ Roadmap to Secure Control Systems in the Energy Sector
 - Partnership between DHS and DOE
 - Should be released 1st quarter 2006
 - Guidelines, not requirements [yet]
- ❑ NIPP
 - National Infrastructure Protection Plan
 - DHS would operate Sector Coordinating Councils and Government Coordinating Councils
 - DHS will set sector-specific goals



Regulatory Compliance

- ❑ Auditors, lawyers and state utility boards/commissions are watching closely
- ❑ The 3Ps...
 - Policy
 - Process
 - Procedure
- ❑ Documentation is your **best friend**
- ❑ Seek “Common Practices” from peers
- ❑ There are things worse than sanctions...



Security Organization

- Organizational Structure
 - Best Practice: outside of IT (fox and henhouse)
 - Business culture and “tone at the top” matters
- Convergence is the trend
 - IT Security
 - Information Security
 - Physical Security
 - Disaster Recovery
 - Business Continuity Management
- Security maturity
 - Move from reactive to proactive
 - Measure security to show effectiveness



Security Spending

- ROI (or ROSI)
 - Is it a myth?
 - ALE and friends
- Technology
 - Security is a process, not a product
 - APS: Aware Person System
 - More devices isn't always the answer
- Services
 - Outsourcing is risky, for many reasons...
 - Be very specific in your SOWs and contracts



Best Security for the Buck

- Patch Management
 - Don't forget to test before implementing
 - ***Be careful with Control Systems...***
- Change Management
 - Use technology and strong [auditable] processes
- Security Awareness
 - Everyone should actually want to be secure
 - Remember, you are in the Critical Infrastructure
- Third-Party Assessments
 - Get an expert opinion
 - Look at different technologies/processes often



Putting it all together...

- Understand your security position
- Think of things in terms of Risk
- Set clear policies and procedures
- Get control of patches and changes
- Educate and raise awareness
- Be aware of changes to the landscape
- Measure and report for success



Utility Management Certificate
Atkinson Graduate School of Management



Questions?

Patrick C Miller CISSP-ISSAP, SSCP, NSA IAM

- Sr. Information Security Consultant
- PacifiCorp Corporate Security
- patrick.miller@pacificorp.com
- 503.813.7014 (desk)
- 503.709.4678 (mobile)

Stacy J Bresler CISSP, CISA

- Manager, Information Security
- PacifiCorp Corporate Security
- stacy.bresler@pacificorp.com
- 503.813.6430 (desk)



Utility Management Certificate
Atkinson Graduate School of Management

