



**Process Control Systems
Industry Conference**

Industrial Security & Compliance Using the Holistic Lifecycle Model

Clint Bodungen
Founder / Lead Analyst
CIDG, Corp.
(Critical Infrastructure Defense Group)



Chris Paul
Counsel
Joyce & Paul, PLLC



Jeff Whitney
Founder
Berkana Resources



State of the Industry

◆ Security and Compliance

- “IT vs. SCADA”, “Them vs. Us”
- Cyber Security Debate
- Myriad of Standards, Guidelines, and Best Practices
- Current “technical” guidance is very broad
- Lack of “agreed upon” guidance

◆ Potential Downfalls

- Auditor Interpretation – Failed Audit – Penalties
- Incident – Fines (penalty and compensatory)

Where is the actual threat anyway?

◆ Cyber Security Threat – Real or Hype?

- If there is no hard-core evidence of a significant [outside] cyber attack, where is the threat?
 - Is there an actual threat? Yes.
 - Is it as great as some claim? Probably not.
- Increasing use of commercial off-the-shelf (COTS) software
 - Existing vulnerabilities
- Connectivity to enterprise
- Increased Exposure
 - DHS' focus
 - Media exposure
 - Terrorist interest (documents found in 2002)
 - Increase in presentations at “Defcon” and “Blackhat”
- Word is now out

Where is the actual threat anyway?

◆ Physical Security and Operational Security (The “Human Factor”)

- Lack of focus
- Common responses:
 - “Yeah, we know our physical security is weak...”
 - “Not my department...”
 - “Oh well... what can you do...”
 - “Operational Security?”
 - “The standards don’t say I have to...”
- Most current standards, guidelines, and best practices focus primarily on cyber-security
- Physical and operational security weaknesses provided additional attack vectors and access to your cyber-systems
 - 100% success rate gaining access to control systems when also testing physical and operational security

Regulatory Confusion

◆ Regulatory Compliance

- Multiple standards, guidelines, best practices
 - Overlapping
 - Most of these are very broad and lack technical, and community “agreed upon”, guidance
- “Not only *how* do we meet compliance and secure our systems, but what standards are we held accountable to?”
- Certain standards are already beginning to be *enforced* even before issues are resolved
- Liability “trap”

Where are the liabilities? (Facts from the field)

◆ Regulatory Compliance

- Increasing demand
- Increasingly subject to enforcement
- Great significance in any incident where SCADA systems may be a core component of an investigation, lawsuit, or regulatory enforcement action
- Failures have resulted in bad press, large fines, and jail time.

◆ Interpretation

- Shift in liability
 - Knowledge and obligation to understand can now fall on operators and management
- Potential for charges of negligence being changed to allegations of willful misconduct
 - Criminal liability
 - Increased civil exposure

Where are the liabilities? (Facts from the field)

◆ Potential Issues

- Outsider Involvement – “significant to a party outside of the company”
 - Adverse economic impact on a third party
 - “the pipeline went down because of a leak, resulting in a supply disruption”
 - Injury or damage to the environment
 - Injury or death of any person (including an employee)
 - Outsiders will look at the failure of the company
 - FTC, DOT, OSHA, EPA
 - Plaintiff Lawyers
 - 20/20 Hindsight
 - Records, security, policies, procedures, and company decisions

Where are the liabilities? (Facts from the field)

◆ Potential Issues

– SCADA Records

- Will most likely be scrutinized
- Can they be produced?
 - If not, allegations may arise that the company destroyed records or have something to hide
- May come into play during a civil lawsuit
- They will be carefully reviewed to point out problems
 - Compliance
 - Training
 - Manuals and policies
 - Age of the system
 - Physical security
 - Ergonomics
- Even from a 3rd party criminal act, blame could fall on insufficient security

Where are the liabilities? (Facts from the field)

◆ Vendor Exposure

- Subject to subpoena and discovery by regulators and plaintiff lawyers
 - seeking information about the activities on behalf of the operator
- May be subject to legal action
- Best Case: Can plan on having business disrupted
- Worst Case:
 - Can accept liability
 - Become a defendant
 - Blame the customer
 - Cripple business

How do I address all of these issues?

◆ The Holistic Lifecycle Model for Industrial Security and Compliance

- Addresses Compliance, Security, and Operations
- Cross-standard
- Designed for Critical Infrastructure and Industrial Verticals
 - Maximize security
 - Achieve regulatory compliance
 - Minimize Liability
 - Improve interdepartmental cohesion
- Complete set of methods and processes, not just a self assessment, “SVA”, etc.
 - Standards, guidelines, best practices selection
 - Analysis
 - Mitigation and Remediation
 - Legal Support
 - On-going support
- Each phase builds on the other (Lifecycle)
 - Due diligence
- Top-down design to improve interdepartmental cohesion

How do I address all of these issues?

The Holistic Lifecycle Model for Industrial Security and Compliance



How the model works:

- Note: Due to the individualization of the model, much of the technical detail is highly dependent on direct interaction with each individual operator's environment

◆ Phase 1 – Assessment

- “Industry standard” SVA or gap analysis will not ensure security or compliance
 - Could actually create liability
 - Many steps are required to build the necessary due diligence
- Standards Identification and Selection
 - Exhaustive search of all regulatory requirements, standards, guidelines, and best practices
 - Include cross-vertical
 - Narrow down to most applicable
 - Starts the path of due diligence (selections and exclusions)
 - Matrix final results

How the model works:

	A	B	C	D	E	F	G	H	I	J
1	CATEGORY	APPLICABLE INDUSTRIAL SECURITY STANDARDS					INTERNAL POLICIES		Coverage	
2		ISO/IEC 27002	API 1164	CFATS	AGA 12	ISA SP99		SP001	SP002	
3	SECURITY POLICY	3	1.1, 7.1		3, F.2			4.5		X
4	Information security policy	3.1			3.1, F.2			4.5		X
5	Information security policy document	3.1.1	2.3, 2.6, 7.2		3.1, F.2, F.3			4.5		X
6	Review and evaluation of information security policy	3.1.2	B.4.2, B.5.1.5		3.4, F.2			4.5		X
7	VULNERABILITY AND RISK ASSESSMENT	7.1.1, 7.1.5, 7.2.5, 7.2.6						5		X
8	General considerations for conducting a risk and vulnerability assessment		5.1.2, B2		2.4, 3.2, 3.3, F.4			5	4	X
9	Three layer analysis				F.4.1					
10	Security architecture analysis				F.4.2				4.6	X
11	Successive compromise analysis				F.4.3					
12	Quantitative risk analysis				F.4.4.1			5.5		X
13	Qualitative risk analysis				F.4.4.2			5.5		X
14	Risk management process		B.2		3.2, 3.3, 3.4, F					
15	Mitigation program		5.1.2, B.2.3		3.4, F.3, F.5					
16	Equipment backup		5.1.2, B.2.3.5, B.3.5.1						8.1	X
17	ORGANIZATIONAL SECURITY	4	B.5						7.4.5	X
18	Information security infrastructure	4.1	B.5, B.5.1		3.1, F.2				7.4.5	X
19	Management information security forum	4.1.1	B.5.1.5		3.1				7.4.5	X
20	Information security coordination (within the organization)	4.1.2	B.5.1.5		3.1, F					

How the model works:

◆ Phase 1 – Assessment (Continued)

– Policies and Procedures Analysis

- Industry may refer to this as a “gap analysis”
 - This term can create problems
- Internal policies and procedures compared to selected standards, guidelines, and best practices
- Personnel interviews must be performed
 - Clarification and accuracy
- All results are confidential and should be treated as such!

– Critical Asset Identification and Classification

- Requirement for certain industries
- Relatively clear-cut
- All results are confidential and should be treated as such!

How the model works:

◆ Phase 1 – Assessment (Continued)

– Security Vulnerability Assessment (“SVA”)

- Most standards prescribe an “SVA” of some type
 - Mostly focused on “cyber”
 - Typically leave gaps
- Must cover Physical, Cyber, and Operational
 - Even if your governing standards only “seem” to focus on “cyber”
 - Penetration testing
 - “Red-team” testing
- SCADA / PCN approved methods only
- Documentation and communication is critical
 - Could serve as a roadmap for attorneys or agencies to attack you
 - Discussed more in the Legal Phase
- All results are confidential and should be treated as such!

How the model works:

◆ Phase 1 – Assessment (Continued)

– Assessment Validation

- All assessment results must be validated
 - Penetration testing
 - Technical Interviews
- Simply running cyber assessment tools such as Nessus, Retina, etc. is not acceptable
 - Can leave gaps
 - False Positives and Negatives
- Only SCADA or PCN approved testing methods should be used
- Test on non-production systems of like configurations
- All results are confidential and should be treated as such!

– Risk Analysis

- Data gathered thus far must be analyzed
- Risk models and formulas are specific to your industry and organization

How the model works:

◆ Phase 2 – Mitigation and Remediation

- Strategy based on data and analysis from Assessment phase
- Policies and procedures enhanced
- “How do you know that your interpretation of the standards is correct?”
 - **We are not interpreting**
 - We are providing a foundation of due diligence so that interpretation cannot be used against us
 - If you can show that you have performed exhaustive due diligence, in an effort to clarify and satisfy any vague requirements of a particular standard, you should have a solid defense in the event of an audit of possible litigation.

How the model works:

◆ Phase 3 – Validation

- Verifies implemented remediation and mitigation have been deployed and effective
- Revisit Assessment Phase
 - Re-run vulnerability assessments
 - Re-run penetration and red-team tests as needed
- Fine tune strategies, mitigations, and operations
- Regular validation schedule should be implemented

How the model works:

◆ Phase 4 – Legal

- The foundation for establishing due diligence throughout the entire model
- Be aware of potential liabilities
- Personnel are first line of defense
 - Should have in-depth understanding of business and operations
 - Be able to recognize various exposures in the event the system fails, suffers a security breach, or is in compliance violation
- Not theory. Lessons learned from litigation
 - Improperly performing tests and assessments can create liability
 - Improper documentation and communication can create liability
 - Avoid words which give legal opinions, legal conclusions, or characterize conduct
 - Do not guess, especially on cause. Don't use phrases such as: "I feel that . . ."; "I think that . . ."; "I believe . . ."; "I suppose . . ."; or "appears to be. . .". If you do not know, investigate

How the model works:

◆ Phase 5 – Management

- Not just security monitoring such as IDS
- Policy and procedures updates
- Establish a feedback loop
 - Maintain current standards, guidelines, and best practices within the matrix
 - Monitor emerging threats
- Establish a regular testing and assessment schedule
- Top-down buy-in for interdepartmental cohesion

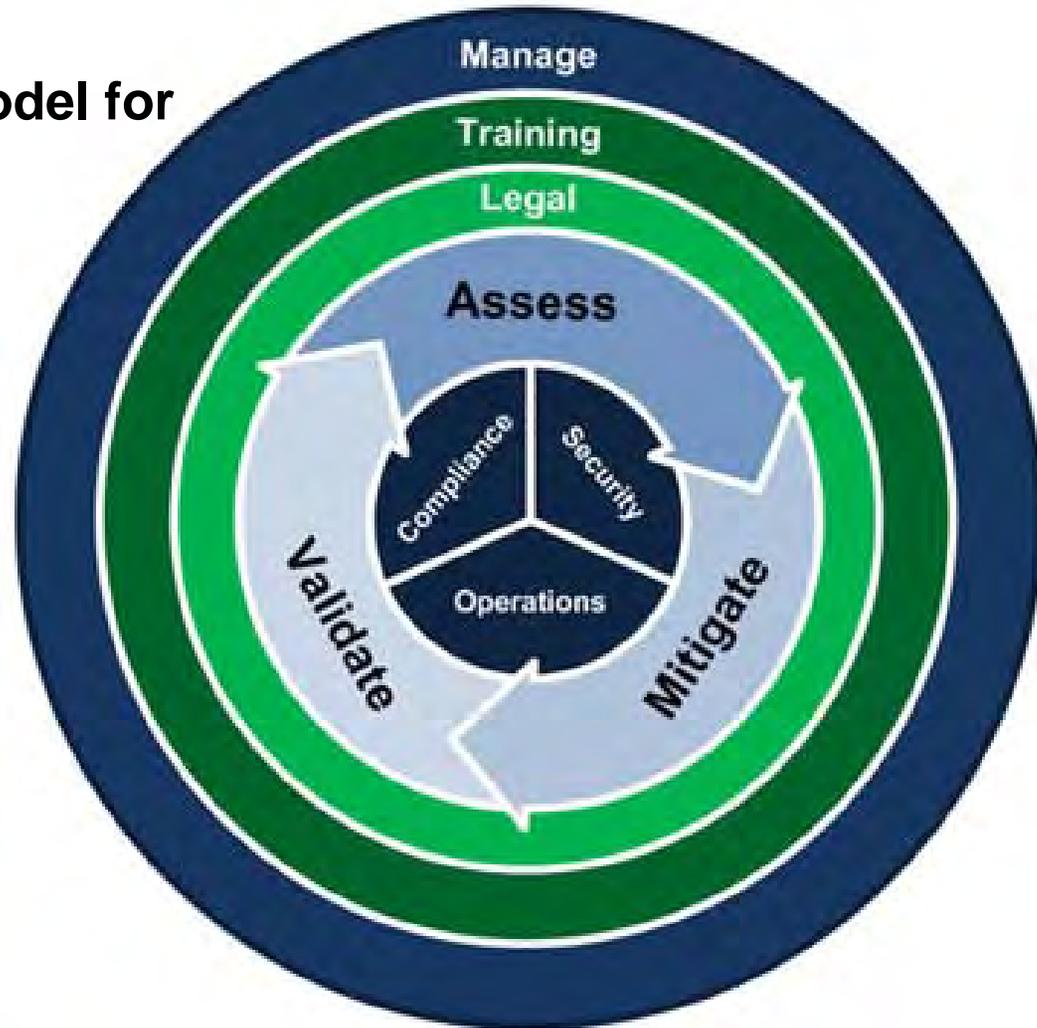
How the model works:

◆ Phase 6 – Training

- Very critical keystone of the entire model
 - If the human element fails, security will unravel at the core
- All stakeholders must understand the strategic objective of the model
- All stakeholders must be trained at their tactical level
- Even though it is referenced in many standards, training is one of the most, if not THE most, neglected aspect of security programs
- Many employees do not remember or adhere to security training given
 - Aspects must relate and pertain to the employees
 - Must be enforced
 - Refresher training and regular exercises are a must

That's it... in a nutshell...

The Holistic Lifecycle Model for Industrial Security and Compliance



Q&A

- ◆ Questions?
- ◆ For more information:

Clint Bodungen
CIDG, Corp.
(888) 384-0969 x801
clint@cidgcorp.com
www.cidgcorp.com



Jeff Whitney
Berkana Resources Corporation
(303) 293-2193
jwhitney@berkanaresources.com
www.berkanaresources.com



Chris Paul
Joyce & Paul, PLLC
(918) 599-0700
cpaul@joycepaul.com
www.joycepaul.com

