



NERC Cyber Security Assessment – Lessons Learned

ERCOT Cyber Security Workshop
November 1, 2006

Jay Abshier, CISSP CBCP
Joseph Bucciero

jay.abshier@kema.com

832.717.0803

joe.bucciero@kema.com

215.997.4500 x206

Agenda

- KEMA Overview
- Determining Critical Assets and Critical Cyber Assets
 - Criteria Based Risk Assessment
- Prudent Cyber Security
- Vulnerability Assessments
- Policy and Procedure Development
- Incident Response
- Recovery Plans
- Compliance Mechanisms
- IT Vs Operations
- Typical Project Phases
- Summary and Key Issues

KEMA at a glance



Serving electric utilities' diverse needs from generation to retail

- Established in 1927, Arnhem, the Netherlands
- Three primary business lines:
 - Consulting
 - Testing
 - Certification
- 1,300 professionals in 18 countries
- Annual revenues of \$200 million

Independent experts to the global utility industry



KEMA consulting expertise

Focused on evolving key market issues

- Operational excellence
- System automation
- Power system automation
- Power systems operations and control
- Power system planning, engineering and protection
- Demand side management
- Sustainable market strategies
- Power generation optimization
- Cyber security of control systems

Vision, proactive strategies, fresh approaches to utility challenges



KEMA consulting expertise

Cyber Security of Control Systems

- Vulnerability Assessments
- Risk Assessments
- Security Program Development and Security Governance
- Policy Development
- Procedure Development
- NERC CIP Compliance
 - Critical Asset and Cyber Asset Determination
 - Gap Analysis
 - Compliance Program

Vision, proactive strategies, fresh approaches to utility challenges



Determining Assets

- Derive list of Critical Assets
 - Risk based analysis using “interpret[ation] and implement[ation]” of “Reasonable Business Judgment”
 - Power System Operationally based
 - “Consideration” of specifically named asset classes
- Common elements of most Risk Assessment Methodologies
 - Assume the target – the critical asset – is already determined.
 - Apply probabilities (quantitative or qualitative) to threats to and vulnerabilities of these assets. But, for CIP the asset is either critical or not critical – not a probability.



Determining Assets

- CIP is concerned with Risk to the reliability and operation of the Bulk Electric Grid
 - Is the Bulk Electric Grid at Risk if this asset fails to function? Yes or No – really a criteria based risk question.
- What criteria (asset classes)?
 - Control Centers
 - Transmission Zone Interconnection Lines
 - 500 kV Lines
 - Outage Transfer Distribution Factors
 - Bulk Generation Support
 - Black Start Facilities
 - SVC Facilities
 - Special Protection Schemes
 - Topology (Assets Linking Critical Assets)



Determining Cyber Assets

- Derive list of Critical Cyber Assets
 - Communications characteristics: routable protocol or dial-up accessible
 - Similar to Business Continuity questions:
 - What are the key business functions?
 - What cyber assets are required to fulfill those functions? Is the answer time dependent?
 - What other cyber assets are required by the critical cyber assets?
 - Establish Electronic Security Perimeter
- Senior Management approval
 - Annual review
 - May determine null set of Critical Assets and/or Critical Cyber Assets



Prudent Cyber Security

- Question: “If I have determined that my entity is NERC CIP auditably compliant, have I done everything I need to do?”
- Answer: “Maybe, but not necessarily.”
 - There is no requirement that assessments be done by outside agents. But, is that prudent?
 - There is no requirement that penetration attempts be made from the Business network into the SCADA/Control System network. But, is that prudent?

Vulnerability Assessments – Lessons Learned

- Lack of or insufficient Control System tailored Cyber Security Policies
- Lack of or insufficient Control System tailored Cyber Security Procedures
- Lack of sufficient training or awareness
- Lack of sufficient Incident Response plans
- Firewalls between business and control systems networks have rules that allow intruders in.
- Default passwords on open and non open system devices.
- No rules regarding allowing computers from the outside to physically connect inside the perimeter.
- Control room doors propped open.

Cyber Security Policies – Lessons Learned

- Those that exist are too verbose.
 - No one reads them.
 - Cannot be easily referenced.
 - No one knows they exist.
 - Combine Operational and Technical Level.
- Should be organized or referenced to a standard
 - NERC CIP or ISO 17799?

Cyber Security Policies – Lessons Learned

- Functional Topics (using ISO 17799:2000):
 - Policy Review and Approval
 - Acceptable Use
 - Security Awareness and Training
 - Organization and Governance
 - Classification of Assets
 - Personnel Security and Incident Response
 - Physical Security
 - Communications and Operations
 - Access Control
 - Systems Development and Maintenance
 - Disaster Recovery and Business Continuity
 - Compliance
 - Exceptions to Policy

Cyber Security Procedures – Lessons Learned

- Very rarely are they documented, if they exist.
- People involved very diligent and concerned with safety and reliability – but just didn't think written procedures for computing assets were important - always because of small number of people involved.
- Biggest problem from a cyber security perspective is usually Change Management.

Cyber Security Procedures – Lessons Learned

- For Control Systems, some key procedures include:
 - Access Control
 - Access Authorization
 - Classification of Assets
 - Change Management
 - Recovery Plans
 - Incident Response
 - Policy and Procedure Review
 - Asset Identification
 - Electronic Security Perimeter Access Points

Incident Response Plans – Lessons Learned

- Very rarely exist.
- No scenarios developed and tested to ensure that on-site personnel know what they can and cannot do in responding to an incident.
- No formal decisions made as to team membership or when team membership changes.
- No formal decisions on who can declare an “incident” has occurred. Key difference from IT is that there are regulatory reporting requirements for an “incident”.

Recovery Plans – Lessons Learned

- Very rarely does a plan exist.
- Very rarely is a plan documented when it exists.
- Even more rarely has a plan been tested.
- IT needs to be aware that traditional Disaster Recovery Plan for some Operational assets are not practical
 - Power Plant is a key example

Compliance Mechanisms

- Auditably Compliant is ultimate goal. This requires the existence of documents that prove that process and procedures are being followed, as well as that they exist.
- But, NERC CIP does not dictate HOW.
 - Manually generating these documents and signing them is perfectly ok, but is it practical?
- Automating the compliance mechanisms is advisable, but no one tool is going to be enough.
 - Change Management
 - Configuration Management
 - Patch Management
 - Document Management

IT Vs. Operations

- Background
 - Computing devices in Operations used to be non-routable, proprietary based protocols and operating systems.
 - Now TCP/IP is being installed, and key servers and HMI devices are now Unix and Windows based.
 - Operations computing infrastructure is beginning to look a lot like the IT infrastructure.

IT Vs. Operations

- The IT Perspective
 - Security charged with protecting a chaotic environment
 - New devices, new users, new software require hard fought for rules that everyone must follow:
 - Unique user IDs
 - Complex passwords
 - Password protected screensavers
 - Rigorous patch and change management
 - Lifespan of devices is very short – 3 or 4 years.
 - Implementing these rules causes inconvenience, and rarely is non-conformance justified.
 - Need to protect our systems from Operations.



IT Vs. Operations

- The Operations Perspective
 - Without efficient Operations, your company would not exist
 - Under pressure to keep expenses very low
 - Primary goal is stability, reliability.
 - Result is the lifespan of control systems is very long – maybe decades
 - Lag time from release of a patch to approval to install is orders of magnitude longer than IT – many times systems are version locked.
 - Legacy systems will be there for many more years – systems that do not support “security”
 - User IDs sometimes conflict with reliable operations



IT Vs. Operations

- Resolution
 - Terminology
 - Go to lengths to make sure everyone defines a term the same.
 - “More Secure”, “Configuration Management”
 - Learn each others constraints
 - Isolation and defined trust

Typical Project Phases

- Phase 1
 - CIP 002
 - Determine Methodology for selecting Critical Assets
 - Select Critical Assets
 - Determine Methodology for selecting Critical Cyber Assets
 - Develop Inventory of Cyber Assets for Critical Assets
 - Select Critical Cyber Assets
- Phase 2
 - CIP 003 – 009
 - Determine Electronic and Physical Security Perimeters
 - Do Gap Analysis between current state and that needed for NERC CIP Compliance



Typical Project Phases

- Phase 3
 - CIP 003 – 009
 - Develop Policies and Procedures required for compliance
 - Upgrade infrastructure required for compliance
 - Develop Compliance Mechanisms for proving compliance
- Phase 4
 - Collect required documentation for one calendar year

Summary and Key Issues

- NERC CIP 002 says to use a “risk based assessment methodology”, but do they really mean a traditional risk assessment methodology must be used?
- What is prudent and based on due diligence?
- Are automated tools needed?
- Does IT cyber security and Operations really understand each others constraints and needs?
- Operations will have devices for many years to come that are TCP/IP enabled and do not support “security” features



Questions?

jay.abshier@kema.com

832.717.0803

joe.bucciero@kema.com

215.997.4500 x206