KANSAS CITY BPU
THE POWER OF COMMUNITY

How I Learned to Stop Worrying and Love Cyber Security

Or We have a CIP Audit scheduled ….

Now what do we do?

Bobby Gray

BPU NERC Compliance Officer

Humble Citizen of the Free State of Kansas

Disclaimer

The material included in this presentation is provided in summary and does not purport to be complete. Information presented should not be considered as advice or recommendation to others and before acting on any information please consider the appropriateness of the information to your specific situation.

This presentation contains backward-looking information that may include statements that demonstrate a belief, intent or possible expectation that future conditions may or may not be extrapolated from these representations of historical facts.

While due care has been taken to prepare and present this information, the presenter does not assume any obligation or duty to ensure the factual nature or provide evidence that proves or disproves its factual nature.

All information displayed or discussed during the commission of this presentation is based upon factual experiences and is not intended to mislead or misrepresent the audience, nor cause any unreasonable risk of or actual injury or harm…

However, all content and statements made are exclusively attributable to the presenter and do not bear any burden or assignment of blame upon the presenter's employer (who has not been provided the opportunity to review this presentation in advance of this performance).

No animals or persons acting like animals or masquerading as animals, intentional or otherwise, were harmed in any way during the preparation or commission of this presentation.

Past Performance

- Past Performance is not a Reliable Indicator of Future Performance
  - Unless you are an auditor, then whatever the entity has said or done may be held against you in an Audit
- Poor “Past Performance” does not have to be repeated
  - Sometimes it may be unavoidable or unintentional
- Everyone wants to be “PERFECT” or at least have no Potential Violations
  - Close enough for jazz

Pre-Audit External Reviews

- Sometimes being too close to the data may blind you to gaps, issues, failures or even successes
- Having an outside set of qualified eyes review your evidence can be very enlightening
- The Entity decided to schedule not 1 but 2 external audit reviews from 2 separate entities
  - Because we had so much free time on our hands
  - It was also a good idea
- Eventually this became 2½ external reviews
- Cost of services was not that expensive (<$80k total, including onsite meals) and the value added well exceeded the cost

External Audit #1

- Network & Security Technologies (N&ST) – March-April 2017
  - Why? Partly because the SPP RE suggested them as a good resource (occurred during settlement negotiations for a previous CIP Audit)
- A mini-mega data request from N&ST kicked off the process
  - NERC CIP Reliability Standards CIP-002 through CIP-011
  - N&ST performed an offsite evidence review for 1 week
  - An onsite “Mock Audit” followed this evidence review
  - Risk of non-compliance was measured based on:
    - Documented policies for meeting Requirements
    - Documented policies that implemented the policies
    - Evidence of execution of the documented policies
    - Subject Matter Expert (SME) knowledge of all of the above criteria and handling of exceptions

External Audit #1 Observations

- RSAWs were new and need to be moved past “first draft” to be truly assessed (guidance provided)
- SME’s didn’t have documented processes in place (Tribal knowledge)
- Difficult to judge compliance based on evidence supplied:
  - Missing procedures from evidence or processes are still being drafted
  - Policies missing key words
  - Evidence of execution “usually looks good”
  - Auditor unable to account for “all device types” without boundaries
  - Some key elements not defined
  - Auditor forced to “find evidence” instead of being led to a conclusion that KCBPU is compliant

External Audit #1 – Entity Response

- We're in trouble with a capital "T" and that rhymes with me
- Fear and concern was rechanneled into an intense period of policy and procedure reviews to correct gaps and other issues (all hands on deck)
- EXAMPLE (this may seem trivial):
  - The PRA policy specified that a background check is required every 7 years
  - So what's wrong with that?
  - A more complete and appropriate statement would be:
  - "A 7-year criminal history and background check shall be completed no later than every 7 years."
  - Is there really a difference? Why take the chance?

External Audit #2

- Proven Compliance Solutions (PCS) – June 2017
- **The mock audit analysis performed off-site included:**
  - *In-depth technical reviews of all applicable RSAWs and associated provided evidence*
  - *Listing of gaps identified or recommendations for improvement using supplied RSAWs*
  - *Scheduling of on-site interviews*
  - *Generation of questions for on-site SME interviews*
  - *Issuance of Data Requests (DRs)*

External Audit #2 Observations

- SMEs provided responses to data requests in a timely manner
- RSAW descriptions for many requirements need more detail describing processes and systems used to meet compliance. BPU should walk the reader through a short example of how it complies with the requirement and point the reader to the applicable page or section in the procedure. Some evidence documents referenced in RSAWs were not supplied with the initial evidence.
- Plan, program, or process documents should be developed, where required, in addition to policy documents
- PDF files provided should be searchable and signed
- SMEs were able to quickly locate Cyber Assets during the inventory process
- Excellent PSP borders and access controls (including defense in depth approach)
- Excellent escorting practices

External Audit #2 Recommendations

- PCS recommends adding an audit prep quality control check of RSAWs and documentation to insure internal review comments and tracked changes have been removed prior to initial submittal and responses to DR's. The submitted RSAW and/or document should be the latest clean copy intended for submittal.
- PCS recommends continued development of internal process to improve tracking of latest RSAW version and policy/plan/procedure documents.
- PCS recommends performing a quality control review for responding to all DR questions.
- If a DR contains more than one question, PCS recommends providing a summary document describing which evidence files correspond to which Question.

KANSAS CITY BPU
THE POWER OF COMMUNITY

Next Steps

- More collaborative document reviews performed internally
  - EMS Staff
  - Compliance Staff
- Focus on feedback from both External Audits
- Ensure that procedures were coordinated with policies and demonstrated implementation of the policies
- Do we really have everything covered now?
- CONCLUSION
  - We think so, but it couldn't hurt to have the first external audit review the current state of the documentation after completion of the 2 external audits (External Audit #2.5 – July 2017)

BPU Observations and Conclusions

- External reviews found no “severe” gaps, mostly strengthening of existing policies, procedures, plans, etc. and the implementation of these documents
- Forced the entire team to work together. BPU adopted a healthy level of stress in the review meetings and encouraged all team members to express their comments and opinions
  - “Put everybody in a room and don’t come out until everyone can agree on the final product.” (requires compromise and respect)
- Strong preparation for the EMS-Team, most of whom had not actual CIP Audit experience

The CIP Audit is coming! The CIP Audit is coming!

- The efforts of the external auditors and the BPU team members will now be put to the test
- Entered the data request phase on August 11
- By September 22, BPU had submitted 1,000+ evidence files
- As of October 19 BPU has responded to:
  - 57 Evidence Questions
  - 15 Evidence Requests
  - Held 3 conference calls with the SPP RE Audit Team
  - Majority of questions and requests are minor issues and appear to be more toward educating the Audit Team

To Be Continued

- The onsite CIP Audit is scheduled for:
  - Week 1 – November 13-17, 2017
  - Break for Thanksgiving (and hope Week 2 is not needed)
  - Week 2 – November 27-December 1, 2017
- BPU is cautiously optimistic but the substance of the EQ and ER from the offsite audit by SPP RE is a cause for concern
  - "What is "Carbon Black" and what is it used for in the BPU environment and where does it reside?"
  - "Reference the pre- and post- detailed and summary patch reports submitted with Evidence Request 11. Please explain what the **red "x"** and **green check mark** means as associated with a specific update."

KANSAS CITY BPU
THE POWER OF COMMUNITY

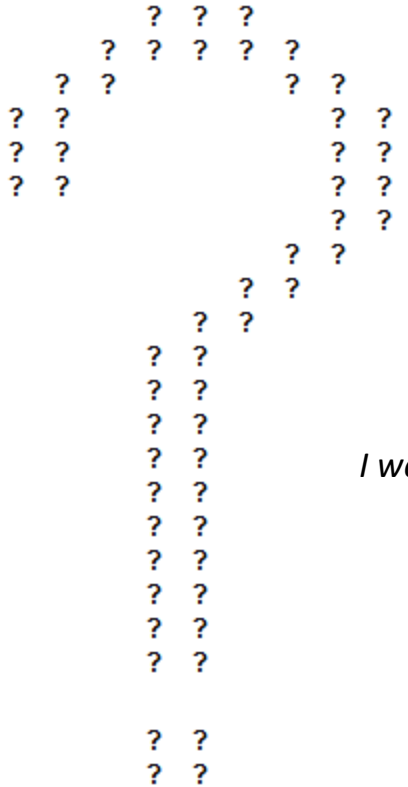
Questions

You're killing me Smalls!

We'd all love to see the plan

Too much time on my hands

My heroes have always been cowboys



Wasted days and wasted nights

I wouldn't say I've been missing work lately.

Work expands to fill the time available for its completion