NPCC

Top Violated Standards Webinar

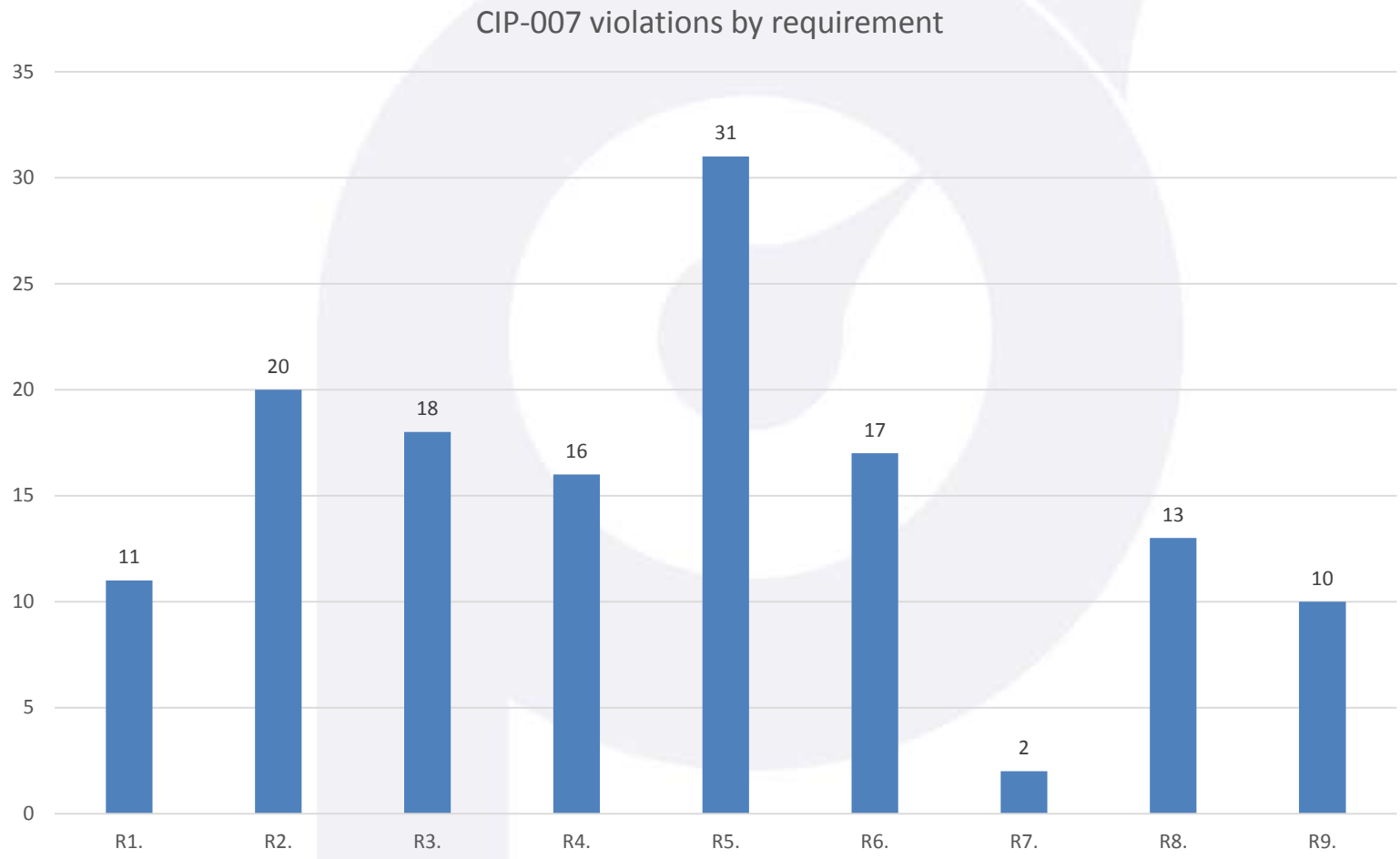
Analysis of 3 violations

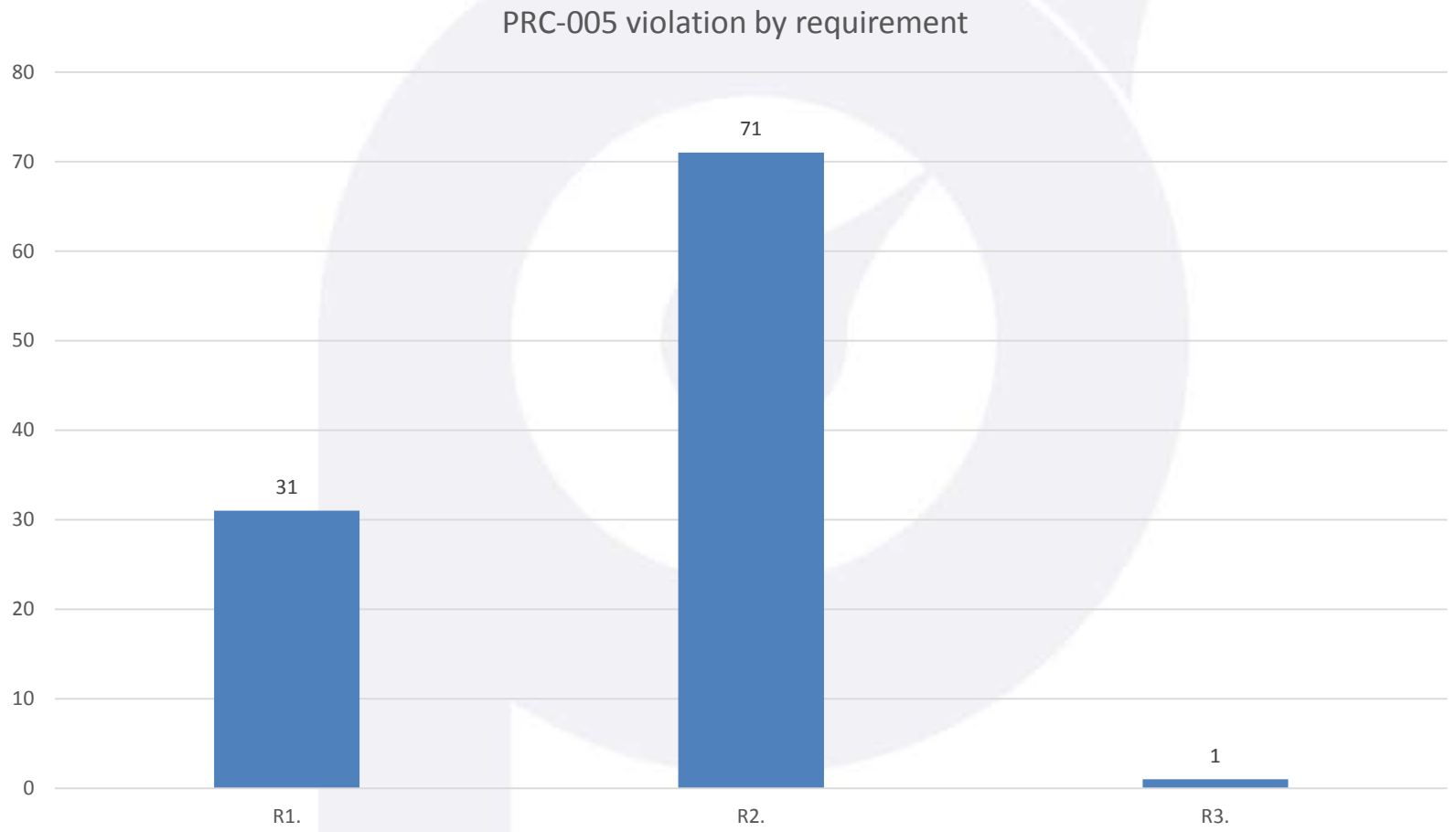
1. Description
2. Contributing factors
3. Lessons learned
4. Risk assessment

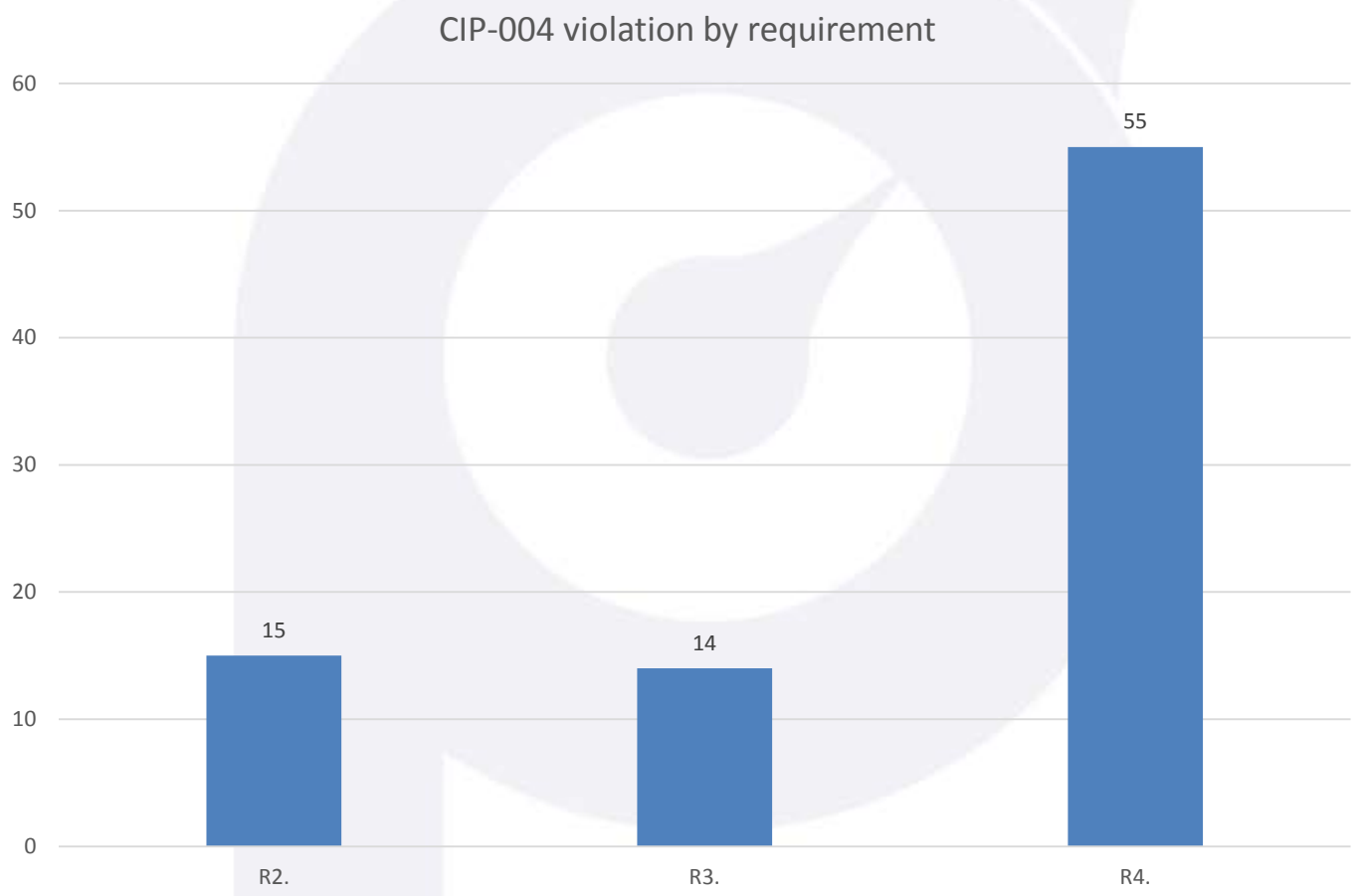
Objectives

- Provide you with a better understanding of risk associated with violations
- Preparing effective Mitigation Plans
- Internal Controls

Standard	Noncompliance
CIP-007	138
PRC-005	103
CIP-004	84


CIP-007 violations by requirement
35
30
25
20
15
10
5
0
11
20
18
16
31
17
2
13
10
R1.
R2.
R3.
R4.
R5.
R6.
R7.
R8.
R9.


PRC-005 violation by requirement
80
70
60
50
40
30
20
10
0
31
71
1
R1.
R2.
R3.


CIP-004 violation by requirement
60
50
40
30
20
10
0
15
14
55
R2.
R3.
R4.

Registered Entity

- GO/GOP
- Large entity

CIP-007 R3

Violation duration: 3 and half years.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and *implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security* Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

Description of Violation

- Entity failed to properly and completely follow the corporate patch management program for Window devices and procedures for non Window devices.
- They could not demonstrate that they assessed patches for applicability within thirty days of the availability of the patches for certain patches.
- During an audit it was determined that they failed to implement a security patch management program for tracking, evaluating , testing and installing applicable cyber security software patches for all Cyber Assets within the ESP.
- Specifically the entity was unable to demonstrate that it assessed patches for applicability for Windows, business servers, Network SCADA and other applications within thirty calendar days of the availability of the patches.
- Also for a Cyber Asset that was not technically feasible to patch, they failed to document compensating measures to mitigate the risk.

Contributing Factors

- Entity faced difficulty in information management and planning activities
- Did not have effective information management practices
  - Did not have enterprise wide protection of information assets through physical, technical and administrative controls.
  - Resulted in delay in remediating noncompliance due to inability to efficiently make and implement decisions across the organization.

Root cause

- Entity did not implement what was documented.

- Standard requires *implementation* of security patches and not only establishing and documenting the program.
- By not patching as required , entity was implicitly accepting the risk involved in not patching cyber security patches for all Cyber Assets within the ESP.

Risk assessment

What is the risk associated with not implementing your patch program?

Minimum
Moderate
Severe

What are some mitigating actions you would take?

Registered Entity

- GO/GOP
- Large entity

PRC-005

Violation duration 5 years

R1. Each Transmission Owner and any Distribution Provider that owns a transmission Protection
System and each Generator Owner that owns a generation or generator interconnection Facility
Protection System shall have a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES. The program shall include:
R1.1. Maintenance and testing intervals and their basis.
R1.2. Summary of maintenance and testing procedures.
R2. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation or generator interconnection Facility Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Entity on request (within 30 calendar days). The documentation of the program implementation shall include:
R2.1. Evidence Protection System devices were maintained and tested within the defined
intervals.
R2.2. Date each Protection System device was last tested/maintained

Description of Violation

- Generation Company did not include the verification of CT/PT/CCVT secondary output values to the inputs of the associated protective relays in its protection system maintenance and testing program; also does not verify the proper secondary values and also the wiring continuity and integrity from the sensing devices to their associated protective relays.

Contributing Factors

- Generating Company did not recognize that a gap existed between its PRC-005 maintenance program document for verifying the output from its PT's and CT's to the associated relays.
- The compliance gap was facilitated by vague work steps in the procedures governing relay functional testing. The vague work steps left the intended scope of work subject to interpretation by technicians such that relay input verification was not being performed after relay calibration and functional testing.

Root Cause

- Company did not follow its Preventive Maintenance document which referenced relay input verification
- Company recognized this in 2012 but did not change it documents until 2014.

- Pay attention to detail
- Create explicit process for testing relays so that it can be followed
- Don’t leave process left to interpretation by the technicians
- Put together good internal control program so avoid issues like this
- The violation should have been self reported prior to the audit findings

Risk assessment

What is the risk associated with not verifying the secondary outputs of CT/PT circuits and not performing wire checks?

Minimum
Moderate
Severe

What are some mitigating actions you would take?

Registered Entity

- BA,DP,GO,GOP,RP

CIP-004 R2

R2. Training —The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, ***including contractors and service vendors***, are trained prior to their being granted such access except in specified circumstances such as an emergency.

Description of Violation

- R2 Registered entity did not review its cyber security training program for two consecutive years.
- R2.1 Registered entity did not provide evidence contractors and vendors were trained prior to being granted access to CCA's
  - Failed to provide evidence training was conducted at least annually.

Contributing Factors

- Entity has incomplete training documentation.
- Did not follow required timeframes for training
- Entity had multiple process weaknesses in managing cyber security records.

Root cause

- Lack of training.

- Training program in place needs to be updated at least annually
- Contractors and vendors are required to have cyber training prior to gaining access to cyber assets.

- Having weaknesses in managing cyber security issues can lead to lack of awareness of cyber security issues across the organization and its contracted staff.

Risk assessment

What is the risk associated with not reviewing your cyber security program annually and not maintaining evidence that contractors and vendors have been trained?

Minimum
Moderate
Severe

What are some mitigating actions you would take?

Thank you for participating