January 25, 2017

ERO Reliability Risk Priorities Report and Workforce Development

Background

The Reliability Issues Steering Committee (RISC) is an advisory committee to the NERC Board of Trustees. It advises the Board on priorities for issues of strategic importance to Bulk Power System reliability. It is meant to help focus resources on those issues which are of the most critical importance to reliability. For the key risks they examined, they focused on the likelihood of occurrence, the expected impact on reliability, and the trajectory of the associated risks. The RISC released the "ERO Reliability Risk Priorities" report dated in November 2016.[1]

The RISC identified risks as High, Moderate, or Low. The rating is not based on the potential impact to the power grid, but rather whether the risk is understood and there is consensus on how to mitigate and manage the risks. "Cybersecurity Vulnerabilities" were included in the High risk category. The Moderate risk profiles of the loss of situational awareness and physical security vulnerabilities are also impacted by cybersecurity, as well as the Low risk profile of human performance and a skilled workforce. The different risk categories were mapped according to their potential impact and the likelihood of the risk leading to Bulk Power System (BPS) impacts. The cybersecurity area was rated as having the highest potential impact to BPS reliability, and the third-highest likelihood of BPS-wide occurrence.

Lack of Skilled Workforce Identified as a Risk

The report included recommendations to mitigate the risk for each of the risk profile areas. In detailing these recommendations, the RISC missed an opportunity to bring focus to the issue of a cybersecurity workforce talent shortage. For example, the risk profile for "Human Performance and Skilled Workforce" described gaps in skill sets and turnover of key skilled or experienced workers as issues, using the examples of "relay technicians, operators, engineers, IT support, and substation maintenance." Cybersecurity personnel could have been included in that list, especially given the workforce talent shortage for

---

[1] http://www.nerc.com/comm/RISC/Related%20Files%20DL/ERO_Reliability_Risk_Priorities_RISC_Reccommendations_Board_Approved_Nov_2016.pdf

cybersecurity in general, and control system cybersecurity in particular.

The report did specifically mention the lack of skilled cybersecurity employees in the cybersecurity risk profile, with one of the five "Descriptors of the Risk" being, "A lack of staff that is knowledgeable and experienced in cybersecurity, control systems, and the IT/OT networks supporting them (historically separate organizations and skill sets), symptomatic across all industries, hinders an organization's ability to detect and prevent cyber incidents."

No Recommendations for How to Address Workforce Skills Gaps

Although the RISC recognized this problem, the issue was not addressed at all in the recommended mitigation steps. For the cybersecurity risk profile, there were 11 recommended mitigations in the near-term time frame (1-2 years), four recommendations in the mid-term time frame (3-5 years), and three recommendations for the long-term time frame. Exactly zero of these eighteen recommendations dealt with workforce development issues. This omission is even more glaring given the missed opportunity to discuss cybersecurity in the human performance risk area.

EnergySec Workforce Development Programs

Developing a skilled workforce is one of the main focus areas for EnergySec, and we have several programs in this area,[2] ranging from outreach to high school students (long-term impact horizon), partnering with college and university programs (medium-term impact horizon), and technical, security policy, and compliance training for people currently in the industry (short-term impact horizon). While we do not necessarily expect the RISC to specifically mention EnergySec programs, since the report mentioned the problems caused by not having a sufficiently sized and trained workforce, the lack of recommendations for this issue is a major omission.

EnergySec has recognized this issue and been working on solutions for the past few years. We are now scaling up our programs to address this area of risk. For more information contact us at workforcedev@energysec.org or call us at (503) 905-2920.

"A lack of staff that is knowledgeable and experienced in cybersecurity, control systems, and the IT/OT networks supporting them … hinders an organization's ability to detect and prevent cyber incidents."

[2] http://www.energysec.org/workforce-development/