21, rue d'Artois, F-75008 PARIS
http://www.cigre.org

CIGRE US National Committee
2019 Grid of the Future Symposium

IEEE's Task Force on IT/OT Convergence Needs You!

S. KUNSMAN
ABB Inc.
USA

T. L. LAUGHNER
PowerGRID-RX, Inc.
USA

SUMMARY

IT and OT Staff at most utilities are often at odds with one another. There is a new IEEE PES PSCCC Task Force developing a report on how these organizations can work better together. The paper aims to inform the industry about the initiative and is seeking input from both IT/OT staff on what works and what does not.

KEYWORDS

IT OT Convergence, Cybersecurity, IEEE PES PSCCC

theo@powergrid-rx.com

Introduction
In December of 2017, an IEEE PES Cybersecurity workshop was held. Wherein, the need for IT and OT collaboration to enhance utility cybersecurity was identified as a core theme. Even though the need was identified, there remains serious challenges in collaboration between these two organizations within the utility. Consequently, in January of 2019, an IEEE PES PSCC Task Force was created to identify opportunities to bring these two organizations closer, develop a common set of terminology and define roles, and identify the potential common ground. The task force is actively seeking contributions for the Task Force Report currently under development.

The substation forever changed when Ethernet based communication protocols were introduced into automation and control systems. This empowered the utility to connect the control system (SCADA) to the utility administrative network, to other utilities, and to the internet at large. However, this has also exposed the utility control systems to misuse and cyber-attacks.

Originally, regulatory bodies embraced air-gap type technologies in combination with serial communications as the only solution. The deluge of data from substations sensors that is required to support power system reliability improvements has made this an impractical position to maintain. In part, this is also due to the fact that the grid has grown in complexity. Wind and solar generators often have a need to communicate between different utility operations staff.

Risks
In 2015, the Ukraine electric utility suffered from a multi-stage attack that resulted in widespread power outages. In 2016, the Ukraine suffered a second attack on the power system. A key finding in the post mortem analysis was the need for collaboration between utilities, manufacturers in incident response and forensics.

Benefits
The benefits of good cyber security practices are myriad. Measures taken to protect power and automation systems against unauthorized access, attacks, disruption, or loss yields higher reliability for the power system. Conversely, failing to conform to good cyber security practices may result in severe fines from regulatory bodies or worse black outs over significant areas of the power system.

Challenges
While no system can be 100% secure, following best practices will demonstrate due diligence. Threats are constantly changing, and cyber security programs are not free or a one time investment. Arguably, the cost of poor cyber security may be higher. Challenges that plague utilities include organizational, technical, and regulatory issues.

Often times, IT and OT organizations have different challenges they are trying to overcome[1]. For example, in an IT organization, the critical asset being protected is information and confidentiality is paramount, whereas in an OT environment a physical process is the object being protected and system availability is the focus. Risk due to a compromise in an IT cyber security is often information disclosure and financial information, meanwhile in OT, safety, health, environment, and financial issues are at stake. IT generally has centralized servers in well protected data centers. However, OT is generally distributed technology often at remote locations that may be hard to secure physically. IT systems desire availability in the 95-99% range, but control systems have high availability needs in the 99.999-99.99999% (3-5 9's) range. Finally, the response to attacks from both organizations are likely to differ significantly. For example, an IT system might reboot or isolate where OT desires fault tolerance with online repair.

If the technical issues weren't enough, the organizational challenges increase difficulty further. It is rare that a person who is proficient in relay settings and power system control is also a competent server administrator or network security. Similarly, folks who are competent server administrators likely know very little about relays or about protection and control systems in general. Clearly, there

needs to be cross-pollination of skills between these organizations and well-defined roles within the organizations.

Finally, as utilities attempt to address regulatory concerns, governance around cyber security also creates challenges for getting the groups to work more closely together. In addition, the standards for cyber security are ever evolving.

Working Group Effort

There are three tasks that have been assigned to IEEE PSCC TF 9: develop a scope of work, identify a report outline, and conduct a cyber security workshop. The desire of the task force is to engage personnel from both the IT and OT parts of the utility organization. The objective is to identify common ground for the organizations to more effectively secure their respective utility systems and more importantly, have a better understanding of the potential impact behind their decisions. In some cases, it may be that collaboration, particularly in the areas of inventory and incident response may yield some efficiencies. But the group needs to evaluate all links in the kill chain to identify common ground.

Appeal

The WG is in the beginning stage of the work. There is significant need for industry involvement from both IT and OT stakeholders. The proposed outline is similar to the structure of this paper, but clearly elaboration in each section is needed. The following is a list of the proposed sections for the working group report and roughly follow the CIS controls[2]: Inventory, Vulnerability Management, Access Control, Logging, Malware Defense, Data Loss and Protection, Security Awareness Training, Incident Response and Management.

BIBLIOGRAPHY

[1] Working Group IEEE PSCC-S9 Meeting Presentation Materials

[2] The 20 CIS Controls & Resources. Retrieved from https://www.cisecurity.org/controls/cis-controls-list.