Gulf Cooperation Council Interconnection Authority

WORKSHOP
CYBERSECURITY

Newsletter #1

Kuwait, 9 & 10 September 2018

Resiliency & Cybersecurity for Electrical Power Grid

Electric utilities in the GCC region are committed in providing a safe and reliable power supply to their customers. Protecting the interconnected regional grid is vital in achieving this mission. The responsibility of protecting this infrastructure is shared between GCC electric utilities. The expanding cyber-risk requires organizations to develop the ability to resist, react and recover from potentially catastrophic cyber security threats. Electric utilities continually work to protect their systems against cyber attack. However, they cannot focus merely on technology to address cybersecurity. A proactive holistic approach is necessary to develop an effective cyber defense strategy.

GCCIA along with its partners organized this first cybersecurity workshop entitled "Resiliency & Cybersecurity for Electrical Power Grid" with the following objectives:

OBJECTIVES

1. Highlight the sophistication, stealth and persistence of cyber-attacks that organizations are facing today and increase security awareness
2. Share different experiences on this critical issue.
3. To step up GCC members oversight of cybersecurity and to have transparency and collaboration around the subject.
4. Build a network of Champions from each utility

SESSION HIGLIGHTS

The workshop was conducted in two (2) days and divided into sessions where different experts from each utilities collaborate and share their knowledge and experience regarding the subject. Guest speakers with strong background in cybersecurity were also invited to discuss the current landscape and the future of the Cybersecurity in the Power Industry.

MAJOR CYBER-ATTACKS AND IMPLICATIONS ON ELECTRICAL GRIDS

The session highlighted the sophistication, stealth and persistence of cyber-attacks that organizations are facing today and increase security awareness.

INTERNET OF THINGS & CYBERSECURITY EVOLUTION

The session focused on the importance, security and privacy issues, and why iOT security is critical in addition to explaining the evolution of Cybersecurity and its importance.

CYBERSECURITY FRAMEWORK

A cybersecurity framework provides security guidance for how organizations assess and improve their ability to prevent, detect, and respond to cyber-attacks. The session reviewed some of the framework which are used by power utilities to manage risk.

GCC UTILITIES EXPERIENCES IN THE SUBJECT OF CYBER-SECURITY DEVELOPMENT

The session discussed and shared experiences, status and current efforts of the GCC members towards improving electrical infrastructure cybersecurity.

WAY FORWARD TO BUILDING A CYBERSECURITY PROGRAM IN GCC

The session gave an overview of the capabilities that go into cybersecurity program (e.g., threat management, vulnerability management) and which capabilities must be matured first and to what maturity level based on the risks that an organization faces.

Various topics discussed across the session;

- Cybersecurity architecture principles
- Defense in Depth
- Incident response
- Cybersecurity frameworks
- Advance threat protection
- Security policies