J

Invitation & Call for Participation by Israel Electric (IEC)
Cybertech Singapore 27 March 2018
15:00-16:45

Facing ever-growing cyber-attacks of which it may be the favorite target, the critical infrastructure industry must muster the necessary resources to prevent, contain, and eventually manage the cyber events menacing it.

The sophistication of cyber-attacks against us is constantly raising, as each increase of IT involvement and remote actions present hackers with new attackable surfaces and opportunities, and as state-driven efforts and policy implementation in the cyber field are not always enough to prevent critical infrastructures falling prey to cyber-security attacks.

Israel Electric, which bears the responsibility for lighting the whole country of Israel, and boasts resistance to a staggering number of cyber-attacks, brings its experience in this field to create a framework and decision-support guide in cyber crisis situations - the CCM.

CCM = Cyber Crisis Management
Cyber Crisis Management deals with a multitude of aspects and organizational layers: and with decision making, from the IT frontline and up to the C-level.
It also addresses the challenges faced by the highest echelons, from the Board of Directors to the Governmental/ regulatory level, which are particularly relevant to the critical infrastructures market.
Experience teaches that better cyber crisis management greatly minimizes the consequences and damages of probable cyber -attacks on large scale industries, mainly in the critical infrastructures field.

CCM at Cybertech Singapore 2018 by IEC
Cyber-attacks in the past years have negatively impacted not only our daily life, but mainly our conception of the "smart" digital word. It has brought to a new necessity of proficiency and awareness in the various layers of each company or organization. One of the most important layers is the high-level management team, the C-level managers. Their ability to manage a cyber-crisis, based on balanced decision-making and broad understanding of the cyber defense space, is a one of the main success keys to overcome the crisis.
Come to participate and learn from our real-life experience, in a realistic and thrilling workshop designed towards making you, and your organization, more cyber-resilient.

The workshop is geared towards the executive challenges and the financial, legal, PR- related, stakeholders-related and other executive conundrums a Board is faced with in case of cyber-attack. Roundtable chaired by Maj. Gen (Res.) Yiftach Ron-Tal, Chairman of Israel Electric; Moderated by Yosi Shneck, SVP Information & Communication & Chief Cyber Officer at Israel Electric

Agenda

15:00-15:10 Gathering & Mingling

15:10-15:15 Round of acquaintance

15:15-15:45 Virtual organization & attack scenario introduction

15:45-16:20 CCM discussion and attack/defense scenarios development

16:20-16:45 Event summary, Q&A and plans for future activities

16:45 ADDIO

Discussion subjects and dilemmas

- ✓ **Main concern(s) and more concerns - monetary aspect?**
  - Ransomware Pay/ Not to pay? If we pay - will they STOP?
    - **How to pay?**
    -
- ✓ **Organization and management**
  - Whom to call for help?
  - To whom to report?
- ✓ **Whom to inform?**
- ✓ **Who are our allies?**
- ✓ **What is the level of risk appetite, what are the criteria to estimate the risk?**
  - Disconnect external connection?
  - Disconnect critical services?
  - Isolate the whole organization/ move to "stone age" procedures? Or ……
- ✓ **The digital world gaps**
  - Spokesperson - when, where, who, if ?
  - How to respond/use the social networks?
  - Internal policy - employees, board ….
- ✓ **The organizational cyber status picture**
  - What is the "whole picture"? Who can give it to us?
- ✓ Organizational cyber heat map (sensitive areas & issues)

Discussion flow:

- ✓ Maj. Gen (Res.) Yiftach Ron-Tal, Chairman of Israel Electric. Discussion will be moderated by Yosi Shneck, SVP, Information & Communication and Chief Cyber Officer at Israel Electric.
- ✓ The table will be surrounded by additional audience who will have a 10 min. opportunity to present questions to the roundtable participants on a panel-like basis at the end of the discussion.

The IEC CCM Round Table Goal and Outcomes

The main goal of the IEC CCM Round Table is :

-to enable C-level and decision-making executives to "get a taste" of a cyber-attack and be better mentally and organizationally prepared to tackle one, in real life.

-to enable an international group of leading stakeholders, who may wish to continuously update and share the CCM framework based on their ongoing experience, best practices, lessons learned and any additional information.

Event outcomes for the participants:

- ✓ Participation in the future activities of the international group
- ✓ Taking influent role in CCM formation
- ✓ Each participant shall receive a summary of the event's discussions, decisions and lessons learned (to be sent after the convention)
- ✓ Each participant shall receive a summary report including expert analysis, conclusions, and general recommendations for preparedness (to be sent after the convention)
- ✓ New partners and “Comrades in Arms”
- ✓ Exposure to Israel Electric extensive cyberwar experience

Thank you for your participation.

I wish to all of us a fruitful and successful event,

Yosi Shneck
SVP, Information & Communication, CCO
Israel Electric

Join us for an exciting and unique Round Table Workshop.
Whether as a full-fledged participant or as an audience member.
Join those who make a better and safer smart digital world happen

The participation will be for pre-registered participants only! For Registration **iecyber@iec.co.il**

For more information, please contact

.Information Systems & Communication Division - The Israel Electric Corporation Ltd
Tel: + 972-76-8637800 | E-mail: iecyber@iec.co.il | Website: www.iec.co.il/cyber