IEF DIALOGUE INSIGHTS

CYBERSECURITY IN THE GLOBAL ENERGY SECTOR

OCTOBER 2015

www.ief.org

1. Cyber-threats can be grouped into four broad categories: “hacktivism” (individual actors seeking notoriety), criminal (motivated by financial gain), nation-state sponsored actors, and terrorism.

2. The nature of cyber-threats changes constantly, presenting an unprecedented challenge in terms of complexity and potential response strategies.

3. Cyberthreats to the energy sector and critical infrastructure are evolving at a faster rate. To date, neither industry nor government have responded to the cybersecurity challenge to the point where hackers are kept in check.

4. While the energy sector has a long history of successfully overcoming the physical disruption of its infrastructure, the cybersecurity issues resulting from the growing reliance on networked data and industrial control systems (eg. Smart grids, trading platforms, network balancing, and flow rates) presents a very different level of threat. Traditional concepts of energy security need to be revised and considered from a more holistic viewpoint.

5. New cyber-risks will emerge in both the energy and the information technology fields, which are increasingly co-dependent and are likely to blend further as the phenomenon of the Internet of Things (IOT) becomes a reality.

6. Contrary to the intuitive focus on information technologies, it is often the people working inside organisations that are at the core of vulnerabilities in the digital realm. Employees at all levels require greater awareness of the risks from cyber-threats and appropriate training to mitigate them.

7. A “Maginot Line” defense, intended to stop threats before they enter an organisation, is of limited value. Breaches will occur. Resilience is key.

8. CEOs and company boards of directors must take a close, active, and supportive interest in the activities of their cybersecurity teams, not least because investors are paying more attention to this component of corporate strategy when valuing firms and lawsuits follow cyber-breach.

9. The traditional role of Chief Information Officer must be revised to address the growing list of cyber-threats. Specialised security teams, with a much broader range of complementary and specialist skills are required.

10. On a positive note, the appointment of an increasing number of so-called Chief Information Security Officers (CISO) over the last year is an indication that industry is taking action on this last point.

11. Information sharing is among the most effective solutions to addressing cyber threats. Developing shared interests and incentives to improve dialogue and information sharing among energy companies and other related market actors is crucial.

12. The United States has taken the lead in raising public awareness about cyberthreats. However, cybercrime does not respect physical borders. It is an international issue. Proactivity, preparation, and open communication, through information sharing and co-ordination teams will play a key role in addressing the problem.

13. There is a labour shortage in the fight against cyber-threats. Private enterprise can play a leadership role in addressing it.

View the full event and more material here www.**ief**.org