Cyber Security Challenges & Strategies

Abstract

The cyberspace offers a significant opportunity for economic growth and social development. However, concerns about the security of this domain are becoming an increasingly pressing and salient issue. Senior business leaders and government officials placed cyber security risks as having a greater impact than those from terrorism.

In today's world wide digital agenda security is a high concern for governments & citizens as well as industry, businesses & consumers in order to engage in e-government, e-commerce and online services. If these players lack confidence in security, it stands to reason that they may avoid participating in online activities, thereby inhibiting further development opportunities on cyberspace.

To help address this many countries, industries and organizations have started to implement cyber security strategies to ensure that they are somewhat prepared to face serious risks, are aware of their consequences, and are equipped to appropriately respond to breaches in their network and information system. However, for many it is not clear if and how effective their strategies and counter measures are.

A solid cyber security strategy encourages good practices & technologies in information and network security to assist and support in developing strong cyber resilience capabilities, notably by building expertise on security and resilience of industrial control systems, transport and energy infrastructure.

In a nutshell, the main action points to address are:

- Develop standards and norms, legislation (improved regulatory frameworks)
- Enhance strategic collaboration between authorities, industry and academia
- Research, development and innovation
- Counter (cross-) organizational & (inter) national defense activities
- Create a culture of security: inform, educate and raise awareness
- Protect critical information infrastructure
- Defense technologies & services delivered in the cyberspace
- Improved capabilities (processes, tools and coordinating structures)
- Support competence and capabilities building in involved actors
- Perform threat tracking, risk assessment and response
- Warnings, actions and emergency response plans

As different organization are facing different challenges and priorities on resilience, tackling cybercrime, security capabilities, cyber defense, critical information infrastructure protection as well as education & co-operation aspects, this will lead always to individual cyber security strategies and approaches.

High-level speaking, these strategies are influenced by individual inputs, driven by various activities and leading to certain outcomes (short, mid & long term). Anticipated overall impact always being reduced (impact of) cyber crime.