Key Elements to Improve Cyber Security

Eng. Khalid Al Hashmi
Executive Director Cyber Security
Ministry of Information Communication & Technology (ictQATAR)
State Of Qatar
Monday, 1st December 2014
Safeguard National CII

- Assess the risk to CII;
- Implement cyber security controls and standards to mitigate risk to CII;
- Analyze cyber security trends and threats to CII and provide timely reports to stakeholders;
- Foster the use of trustworthy technology products and services; and
- Continuously monitor the security posture of CII
Incident Management

- Enhance and maintain situational awareness capabilities;
- Establish and continuously enhance incident response capabilities;
- Reduce cyber infections within CII;
- Establish mechanisms and procedures to facilitate timely information sharing and action among stakeholders; and
- Ensure preparedness by conducting cyber security exercises and drills.
Legal & Regulatory Framework

- Increase capabilities to combat cyber crime;
- Develop and implement laws, regulations, and national policies to address cyber security and cyber crime;
- Monitor and enforce compliance with cyber security and cyber crime laws, regulations, and national policies; and
- Build and maintain strong international relationships to establish cyber security norms and standards.
Foster a Culture of Cyber Security

- Enhance cyber security awareness across society using multiple channels;
- Encourage individuals to use cyber safety tools and solutions to protect against cyber threats; and
- Promote the development and delivery of cyber security education in schools, colleges, and universities.
Develop & Cultivate National Cyber Security Capabilities

- Develop and maintain a professional cyber security workforce;
- Foster business opportunities and strengthen the competitiveness of the cyber security industry in the public and private sectors; and
- Invest in research to develop and commercialize innovative cyber security technologies and solutions