Minister of Transport, Communications & Works of the Republic of Cyprus

Mr Marios Demetriades

Curriculum Vitae (C.V.)

Mr Marios Demetriades assumed office as Minister of Transport, Communications and Works on 14 March 2014.
Mr Demetriades was born in Pafos on 27 August 1971.
Over the last six years he held a managerial position at Piraeus Bank (Cyprus). Prior to that he worked at Laiki Bank Group for approximately ten years.
He studied Business, Finance and Economics in the United Kingdom (1990-93 University of East Anglia). During his studies he was the recipient of many awards.
Since 2000 he is a member of the CFA Institute (Chartered Financial Analyst).
Since 1996 he is a member of the Institute of Chartered Accountants in England and Wales (Chartered Accountant) and a member of the Institute of Certified Public Accountants of Cyprus (ICPAC).
During the period 1993-96 he worked at the international firm BDO Stoy Hayward in London as a trainee Chartered Accountant.
From 1996 until 1998 he was manager of the Pafos local office of the international audit firm EY.
From July 1988 until August 1990 he served his military service at the National Guard.
Mr Demetriades is married to Maria and they have two children.

Opening address by Mr Marios Demetriades
Minister of Transport, Communication & Works of the Republic of Cyprus

Ladies and gentlemen,

It is with great pleasure to be here, in the second CYpBER Maritime - Oil & Gas conference.

The maritime as well as the oil and gas industries are of major importance to Cyprus. A secure development of their information infrastructures is critical, so that stakeholders and investors can gain the necessary confidence in developing their operations. Both sectors are facing the challenge to safely embrace modern information and communication technologies in their systems. The Cyprus government aims to work with and support all stakeholders including the maritime and energy sectors in achieving their goals and enhance security levels in the provisioning of their services.

Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered directly or indirectly via the Internet by cyber criminals. This has led into a new area of potential maritime threats that go well beyond physical piracy.

Energy is essential to a nation's security, economic stability, and global trade, yet is particularly vulnerable to attacks and disruption in the maritime environment. In short, there are as many potential avenues for cyber damage in the maritime sector as there are cyber systems. While only some cyber-attack scenarios in the maritime sector could credibly lead to a Transportation Security Incident, it is important to identify and prioritize those risks, take this threat seriously, and work together to improve defences.

Cyber security is not only the largest, but one of the critical safety challenges that an oil and gas company can face. With the exploitation of new cost-effective operational concepts, use of digital technologies and increased dependence on cyber structures, the oil and gas industry is exposed to new sets of vulnerabilities and threats. Recent research in the field has revealed that energy companies are actively managing their information security, but just over half (58%) have adopted an ad hoc management strategy, with only 27% setting concrete goals. Security is only as strong as the weakest link. Many times the infrastructure alone is not the weakest element. Employees and executives who are not adequately trained in security threats appear to be a major security risk.

The far-flung geographic locations of energy producers also present a huge challenge, which means that connected technology assets are necessary to assure a wide range of essential servic Some of the most important challenges and vulnerabilities that companies are facing include, the lack of cyber security awareness and training among employees, the remote work during operations and maintenance, the use of standard IT products with known vulnerabilities in the production environment, a limited cyber security culture among vendors, suppliers and contractors, insufficient separation of data networks, the use of mobile devices and storage units including smartphones, data networks between on- and offshore facilities, Insufficient physical security of data rooms and other facilities, vulnerable software, outdated and ageing control systems.

The consequences can be serious and wide-ranging for all sectors. Depending on the target and size of the organization, the financial impact alone can reach millions of euros. Furthermore cybercrime can seriously damage brands, compromise customer confidence, violate compliance mandates, and weaken the ability to generate revenue. The energy sector play's a crucial role in the global economy and is expected to play even more important role in Cyprus economy. Cyber-attacks in this field can endanger public safety by disrupting communications, transportation including maritime, exploration, energy refining, power, and utility services.

An effective implementation of the security strategy is a critical element to achieving innovation and growth. The government of Cyprus is recognising the importance of the effective implementation of a national cyber-security strategy. The Ministry of Communications and Works which has the supervisory role in the Information Society and Cyber security fields in Cyprus is working with the other competent Ministries of the Republic in improving security standards in our country. The national Cybersecurity strategy covers further to network and information security and resilience, the fields of cybercrime, cyber defence and international cooperation in the field of cybersecurity. The activities are coordinated by the Office of the Commissioner of Electronic Communications and postal Regulation (OCECPR).

Since many other sectors rely on ICT as an enabler, should therefore be concerned about network and information security and more widely cyber security. As explained before, a number of specific infrastructure and service providers are particularly vulnerable, due to their high dependence on correctly functioning network and information systems. These sectors play an essential role in providing

key support services for our economy and society, and the security of their systems is of particular importance to the functioning of the market. These sectors include banking, stock exchanges, energy generation, transmission and distribution, transport (air, rail, maritime), health, internet services and public administrations.
These sectors are covered under the actions of the Cyber security strategy and more particularly under the national Critical Information Infrastructure Protection (CIIP) framework. The work in this field is underway and will cover the maritime and the energy sectors which are considered as critical.

Ladies and Gentlemen,

In a country like Cyprus, where the economy depends heavily on the supply of services and where the successful exploitation of the opportunities from oil and natural gas exploration is evident, a high level of network and information security and cybersecurity, is important, and will contribute to the development of the required market environment and trust, to enable the progress of our society. The active implementation of the national strategy on Cybersecurity shows the government’s will, to work closely with all stakeholders and help all critical sectors, including the energy and maritime sectors, in order to lead our society to progress and economic prosperity.

I wish you every success in today's conference and I believe that this event will contribute positively towards implementing cyber security practices, proactively and effectively in the all critical fields of maritime and oil and natural gas industry.