Permanent Secretary,
Ministry of Energy, Commerce, Industry & Tourism of the Republic of Cyprus

Dr Stelios Himonas

Curriculum Vitae (C.V.)

EDUCATION
PhD in Electrical Engineering, December 1989
State University of New York at Stony Brook, Stony Brook, New York, USA
Master of Science in Electrical Engineering, December 1986
State University of New York at Stony Brook, Stony Brook, New York, USA
Bachelor of Engineering in Electrical Engineering, May 1985
State University of New York at Stony Brook, Stony Brook, New York, USA

EXPERIENCE
Permanent Secretary
Ministry of Energy, Commerce, Industry and Tourism, Cyprus (04/13 – present)

Permanent Secretary
Ministry of Justice and Public Order, Cyprus (04/12 – 04/13)

Director of Department of Electronic Communications
Ministry of Communications and Works, Cyprus (1/03 – 03/12)

Director of Telecommunications
Ministry of Communications and Works, Cyprus (2/00 – 12/02)

Senior Telecommunications Officer
Ministry of Communications and Works, Cyprus (1/98 – 2/00)

Professor
Department of Computer Engineering, Intercollege, Cyprus (9/97 – 1/98)

Associate Professor with Tenure
Department of Electrical Engineering
New York Institute of Technology, New York, USA (9/94 – 9/97)

Assistant Professor
Department of Electrical Engineering
New York Institute of Technology, New York, USA (9/89 – 8/94)

Visiting Research Scientist – Multimedia Communications
Bell Communications Research (Bellcore), New Jersey, USA (5/94 – 7/97)

RESEARCH
Author of 35 research papers in refereed journals and conference proceedings

HONORS
Member of Sigma Xi Research Honor Society
Member of Eta Kappa Nu Electrical Engineering Honor Society
Member of the New York Academy of Sciences
Who is Who in the World
Who is Who in American Education
Who is Who Among Human Services Professionals
Who is Who in the East

ACTIVITIES
Digital Champion of Cyprus (10/12 – present)
Appointment by the Council of Ministers of the Republic of Cyprus
Member of the Board
Research Promotion Foundation (12/09 – 03/12)
Vice Chairman CEPT/ECC (06/11 – 04/12)
Chairman CEPT/ECC/WGRA (05/06 – 12/12)
Member of the Board
Cyprus Telecommunications Authority (8/00 – 7/03)
Reviewer of research papers submitted for publication to IEEE Transactions on Aerospace and Electronic Systems (USA), IEE Proceedings-F (UK) (1989 – 1997)

Address by Dr Stelios Himonas
Permanent Secretary,
Ministry of Energy, Commerce, Industry & Tourism of the Republic of Cyprus

Honourable Minister,
Mr. Mayor
Distinguished guests,
Ladies & Gentlemen,
It is my pleasure to be here today to welcome you at the «CYpBER 2016» Conference.

I am sure that the other speakers will cover the general issue of cyber security quite extensively. So, I will focus my remarks on the energy sector.

Today the Conference has gathered experts of the sector from all around the world. This is a great opportunity to exchange knowledge, experiences and information about the ongoing cyber threats as well as the means to protect the industry.

During the last decades, Operation Technology (OT) has experienced a significant development and many new intelligent systems have been made readily available for Industrial Control Systems (ICS), offering more capabilities, like IP networking, Remote Access from both Control Center and Field devices, providing increased production speed, control and process efficiency.

These advances however, provide more opportunities to attackers.

There are many types of cyber-attacks: espionage, sabotage and denial or disruption of service. These attacks can have the same or even worse effect and damage as military attacks. Such incidents may cause the loss of life while at the same time keeping the anonymity of the attacker.

Cyber-attacks against the Energy Industry have been on the rise over the last 5 years, becoming more complex and sophisticated.

These cyber-attacks target both Information Technology (IT) Systems and Operation Technology (OT) Infrastructures. The US Department of Homeland Security says that it is the most attacked industry.
According to some reports, the systems of the United States Department of Energy were breached more than 150 times between October 2010 and October 2014. Just before Christmas, regional Ukrainian power companies reported that they had suffered outages after outsiders remotely tampered with their automatic control systems.
It is evident that the proper functioning of our critical infrastructures is a necessary pre-requisite for a healthy economy and the well-being of our citizens.

In Cyprus, we have not experienced until today (at least we don't know about it) any major cyber-attack. We shouldn't however sit back and relax. It only needs to happen once and the results could be devastating. Unfortunately, if we have an incident, the recovery process is both lengthy and costly.

I am sure that the Telecomms Commissioner will explain the national plans of Cyprus with regard to protecting our national infrastructures as well as the country's response plans.

I want to focus a little bit on the oil&gas sector which is at its infancy here in Cyprus. Offshore oil&gas exploration started in 2008 and is becoming more and more intense. As you all know we have licensed 5 Blocks in the Cyprus Exclusive Economic Zone and we have recently announced another licensing round for 3 more Blocks. We are also moving to production as we are discussing the monetization of the Aphrodite gas discovery with the Block 12 Contractor.

It has been reported that in 2015, the majority of oil and gas industry firms (more than 82%) were targeted by cybercriminals. More than half (53%) of these companies state that they experienced an overwhelming upsurge in attacks.

Cyber-attacks on oil&gas activities, if successful, could have severe effects not just on the industry but also on the environment, public health and safety, and even national security.

Analysis has identified multiple points of vulnerability. These are attacks on the industry's physical infrastructure, the disabling of critical systems and the theft or corruption of information or the prevention of its dissemination.

A 2014 report issued by the US Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) suggested that we should combat these threats through boundary protection, information flow enforcement, and remote-access control.

Inadequate boundary protection can create avenues that allow outside parties to interface with systems and devices that directly support a company's control processes. Insufficient control of information flows, can allow attackers to establish unsanctioned and damaging communications, using a company's channels, ports, and services. And weak control over remote access, can create many entry points for unauthorized interfacing with a company's control-system devices and critical components.

The oil&gas companies operating in Cyprus must also invest in the development and application of new protection methods to safeguard their operations in the entire value chain, that is corporate, upstream, midstream and downstream activities.

Ladies and Gentlemen,

Bear in mind one thing: The greatest vulnerability is lack of understanding of the issue.

And I am sure that this Conference will increase our awareness about cyber threats, their effect and how to protect ourselves by protecting our critical infrastructures, IT and OT.

In concluding, I wish to thank and congratulate the organizers for this initiative and wish you all fruitful deliberations.

Thank you!