



SECURITY WORLD 2009

“SECURE your organization in an INSECURE era”

KEYNOTES

Overview of Network Security and Data Protection in Vietnam

Dr. Nguyen Viet The, Director, IT Department, General Department of Technology, Ministry of Public Security

The rapid development of web applications and web-based services has solved the cost-cutting pressure for enterprises in current economic recession. However, accompanied with this development are alarming risks for secure network and communication. In order to improve better network environment for online transactions, Dr. Nguyen Viet The will share some Ministry of Public Security's experiences of investigating cyber-crime in practice.

Smarter IT spending in the global economic downturn

Ms. Elaine Lee, Senior Financial Analyst, International Data Corporation-IDC

It is to be expected that all budgets come under scrutiny during economic downturn. However, In 2009 IDC believes spending on Information Security will remain stronger than other IT areas because of compliance and business requirements. Putting a value on information security investments is therefore fraught with difficulties. This requires looking into how much is spent on information security in relation to total IT investment, confidence level of current protection measures and plans for improvement.

End users might opt to conduct risk assessments to prioritize needs. By conducting assessments, end users will factor the most severe vulnerabilities against the criticality of the asset, risk of compliance violations, and business disruptions. By prioritizing security needs, end users will be able security expenditures within the limitations of reduced budgets while keeping IT security personnel fully employed and improving the corporations IT risk posture.

National Security Information Strategy Planning

Mr. Vu Quoc Khanh, Director, VNCERT, Ministry of Information & Communications

According to VNCERT's research, more than 50% of Vietnamese enterprises and organizations haven't paid appropriate attention to information security. Most of these don't have trouble-shooting process, and only half of them are planning to build up the process in the next three

months. Moreover, the reports of attacks are insufficient and lack of professional technology support.

This alarming situation results in an essential demand for a strategic information security master-plan on a national scale. Delivered by Mr. Vu Quoc Khanh, Director, VNCERT, Ministry of Information & Communications, the keynote “**National Information Security Strategy Planning**” will provide an overview on VNCERT Information Security implementation guidelines from governmental administration perspective. In this report, information security ability is defined based on 5 factors: Legal environment, Governmental Administration, Implementation; Technology; and Coordination ability.

Accordingly, the national information security strategy will be implemented in 4 stages: Monitor and identify information security problems, Analysis and timely response, Coordinate to prevent and minimize losses, Disasters recovery. In this report, national information security strategy will be approached by building an national information processing system; updating data in Vietnam security cyberspace monitoring database and being exchanged with those of international databases.

Protecting the Critical Information Infrastructure

Mr. Vic Mankotia, Vice President, Sales & Services – Emerging Technologies, Asia Pacific & Japan, Symantec Corporation

Security, especially in the government sector, has become a complicated topic. In the old days, security was straightforward. Governments had to secure a perimeter, and as threats got more sophisticated, perimeter security became stronger. Much like building a deeper moat around a castle, the use of sophisticated firewalls and intrusion protection and detection allowed governments to protect their assets within their perimeter.

Today's however, the rapidly evolving technology has spawned new and much more sophisticated threats. With access to sensitive data from all points within and outside the enterprise, the old perimeter has disappeared, and perimeter security on its own can no longer fully protect the information assets. The changing nature of security threats has called for a rethink in how governments design and implement security.

Government security approach needs to change to adapt to all these threats. There's also a need to do a multinational coordination and various collaborations between public and private sectors. Ensuring systems and networks are secure is the key to gaining the trust and buy-in of citizens in e-government services.

Strategic view on Justice and Public Safety – Technology platform

Mr. David Gung, Director Justice & Public Safety Asia Pacific, Oracle Corporation

The IT Trends in Law Enforcement agencies (that are mature users of technology) show that existing applications have been developed in silos and the trend is to modernise these applications to enable Law Enforcement agencies to meet the major challenges they are facing today (Organised Crime, Terrorism and Cybercrime). These are of a transnational nature and present different challenges to domestic crime. Integrated intelligence information is required and the sound security measures are required to protect this very sensitive information from unauthorised access. Oracle the information company has the unique verticle enterprise solutions

(sound secure back-end database, middleware and front-end Investigative Case Management applications that can be leveraged to help meet these challenges.