48 PERCENT OF THE COMPANIES BELIEVE THAT THEIR MANAGEMENT HAS NO OR AT LEAST NOT SUFFICIENT KNOWLEDGE ABOUT CYBER SECURITY THREATS.
100 PERCENT OF THE TOP MANAGERS AND MINISTERS WE ADVISE DO NOT ONLY KNOW THE POTENTIAL INDIVIDUAL THREATS RELATED TO THEIR COMPANY BUT EXERCISED MANAGEMENT INVOLVEMENT IN.

CYBERSECURITY AND CYBERCRIME LEGISLATION JUST LIKE POLICIES AND STRATEGIES CAN BE COMPONENTS IN THE FLIGHT AGAINST HARMFUL ATTACKS. WHICH ROLE CAN AND WILL THE DRAFT LEGISLATION PLAY?

MAIN CHALLENGE

How are Cyber attacks carried out? What is the impact? Do existing Cybersecurity strategies of a country cover the risks? Is Cybersecurity a technical issues that system administrators of affected companies will deal with or is there a need for an involvement of the top management and even government? Which decisions require special attention because the might have significant impact? What is the impact on risk management? What policies are necessary? Which institutions within a country need to be involved?

WORKSHOP ON CYBERSECURITY AND CYBERCRIME LEGISLATION

In order to facilitate the discussion about the draft Cybercrime and Cybersecurity legislation, ITU will organize a workshop on 23rd of March 2015 in Bangkok. Part of the workshop will be a Live Cybersecurity Incident Simulation.

The simulations enables the participants to go through a simulation and assess in a very tangible way potential threats with regard to Cyber Attacks. In a 60 minute simulation they will experience a series of complex and realistic cyber attacks, their exposure to risks, the impact of the attack as well as the consequences of their action and response. 1-5 people will be able to actively participate and they have the chance to find out if they are prepared to go on the defensive and if the policy and legal framework will be able to address the challenges. **The simulation does not require technical knowledge – it focuses on management decisions.**

In order to ensure that the simulation is a truly exciting and realistic experience the plot develops interactively. A decision of the protagonists will lead to consequences in the course of the play. In order to guaranty this level of interaction role players can be utilized.

The simulation is designed to meet the expectations of a demanding target audience (high level government officials). It includes various individually designed multimedia components such as short movies, animations and other sophisticated media. Different screens with background information can be set up and provide a realistic “Cyber Operation Centre” feeling.

MODERATOR

The workshop will be moderated by **Prof Dr Marco Gercke** who for more than 10 years advises international organisations (such as UN, EU, ITU, Council of Europe,NATO), governments and large enterprises in questions related to Cybersecurity.He has conducted such simulations for various clients worldwide. He also acted as advisor and trainer related to legal/strategy/policy related issues in the field of Cybersecurity and Cybercrime for companies and governmental institutions in Asia.

The workshop also welcomes **Dr. Hyung-Jun Seo**, Director of Information Security Policy Research of the attached Institute of Electronic and Telecommunication Research Institute. He will share experience of Korea’s cybersecurity policy and some incidents in Korea.

TENTATIVE PROGRAMME

08:00-09:00	Registration
09:00-09:20	▪ Welcome Remarks by Mr. Ioane Koroivuki, Regional Director, ITU Regional Office for Asia and the Pacific
09:20-10:30	**CYBERSECURITY FRAMEWORK** Recent Developments in the area of Cybersecurity, Relevance for Thailand
10:30-10:45	Coffee break
10:45-12:00	**CYBERCRIME LEGISLATION** Cyber-crime Threats, How Legislation can support the fight against Cyber-crime, International best practices
12:00-13:00	Lunch break
13:00-15:30	**CYBERSECUIRTY INCIDENT SIMULATION** Addressing the challenges of Cybersecurity through legislation has great practical relevance for those who are confronted with such challenges. The “Live Cybersecurity Incident Simulation” demonstrates the implications of threats as well as existing or missing coverage of legislation on businesses and government institutions in Thailand. **PARTICIPANTS** Unlike “live hacking“ demonstrations or technical drills the simulation does not focus on technical aspects of Cybersecurity but management skills. It wasdesigned specifically for the high ranking government officials. 1-5 main players will take an active role and act as management board of a company that is under attack. As mentioned above, technical skills are not required.
15:30-15:40	**CLOSING**
16:00-18:00	**CLOSED GROUP DISCUSSION (DIGITAL ECONOMY KEY STAKEHOLDERS)**