# *INCULCATING THE 'CULTURE OF ICT SECURITY'*

*(This article is extracted from an article titled "OECD Guidelines for the security of information systems and networks. Towards a culture of security". OECD publications, No. 81829 2002)*

By

**Noormawati Mohd Nawi and Lt Col Husin Hj Jazri CISSP**

**National ICT Security and Emergency Response Centre (NISER)**

*"To keep a lamp burning, we have to keep putting oil in it".* Perhaps this is what the Organization for Economic Co-Operation and Development (OECD) attempting to do; in order to create a secure and sustainable system and network security, a constant and continuous effort must be imparted at all times. Therefore, the OECD has initiated the guidelines, which are known as "The OECD Guidelines for the Security of Information Systems and Networks." The OECD consists of 30 representatives of member countries whom have collaborated with international business and civil society groups to critically analyze and debated each guideline in great detail.

Adopted in August 2002 and later received global recognition in the resolution of the UN Assembly on 20 December 2002, the guidelines recommended nine (9) principles which are relevant to all who participate in the information security. They are:

### *1. Awareness*

Awareness is the opening key to security since security cannot takes place if we ourselves are ignorant of the subject matter. We must not only aware that security is important but must also aware about things that we can do to enhance security. The state of awareness is where we realize that there are risks and there are safeguards available. The information systems and networks are interconnected thus making them vulnerable to both external and internal attacks. Thus it is important for us to perceive and comprehend the effect of security failures, the possibility of harm caused to others, the configuration and available updates for our systems, its position within networks, good practices and the needs participation from others.

### *2. Responsibility*

We ought to be responsible for our creation. As such it is our accountability to anything that happens or caused to be happened by the information systems and

networks. The nature of systems and networks make us interconnected and this makes everybody's dos and don'ts counts. Whatever one does or does not do will somehow or rather affect the other party. Therefore, we should be accountable to our acts, must always review our own policies, practices, measures and procedures and assess whether these precaution steps are suitable to the surroundings. For example, it is the responsibility of the manufacturer to disseminate to users the appropriate well-timed security information. This may allow them to properly comprehend the security functions together and what they can do to make it secure.

### *3. Response*

The world is interconnected through the systems and networks we invented. Anything transmitted over them will reach its destination at no time. This is what happens if damage is done. It can be widely spread in the blink of an eye. Therefore, a timely and co-operative act is vital to prevent, detect and respond to security incidents. Sometimes it may also involve cross-border information sharing and co-operation on threats and vulnerabilities as well as implementation procedures.

### *4. Ethics*

The ethics and attitude of the users regarding security in information systems and networks have to be drastically changed. In ensuring security, we must be caution that interests of others may be affected by our do and don'ts lists. It is therefore necessary for us to endeavor in earnestness when establishing best practices so as not to offend any legitimate interests of others.

### *5. Democracy*

The security of information systems and networks should be compatible with essential values of a democratic society such as freedom of speech, expression of ideas and thoughts, unrestrained flow of information, the confidentiality of information and communication, and the appropriate protection of personal information, openness and transparency. These democracy ingredients should be upheld at all times when we are taking care of the security aspects.

### *6. Risk Assessment*

Security efforts should not be allowed to gather dust. A constant risk assessment should be conducted to identify treats and vulnerabilities. This must cover the technology, physical and human factors, policies and third party services. The reason for this is to determine the acceptable level of risk and help to determine the

appropriate controls to manage the identified risks by weighing the nature and importance of the information to be protected. Interconnectivity, however, asks for risks from or caused by others to be assessed too.

### *7. Security Design And Implementation*

We should incorporate security as an essential element of information systems and networks by means of designing and adopting the appropriate technical and non-technical safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. These safeguards and solutions must be proportionate with the value of information on the organization's systems and networks. Security must be a vital factor of all products, services, systems and networks, system design and architecture.

### *8. Security Management*

We should adopt a comprehensive approach to security management. This should be based on risk management and includes all levels of participants' activities and all aspects of their operations. Other factors to be included are emerging threats; address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. The information system and network security policies, practices, measures and procedures should be co-coordinated and integrated in creating a coherent security system. What is required under the security management will depend on level of involvement, the role of the participant, the risk involved and system requirements.

### *9. Reassessment*

We should review and reassess the security of information systems and networks and make appropriate modifications to security policies, practices, measures and procedures. This is because the new and changing threats and vulnerabilities will keep on coming. We must always be on guard and ensure that we are security-tight.

To inculcate the culture of security, leadership is very much needed. The appointed leader shall guide and indicate that security should be given a priority in planning and management. This is to be followed by participation across the board ranging from levels of government, business and civil society. Participants should constantly be made understand about security. The nine (9) guidelines and other security drives are to help participants to install security into their design, implementation and use of

all info systems and networks. Each and every user must be treated as the main factor determining the success of this culture.

The ‘C*ulture of Security’* intended to change the mere compliance social pattern into doing things and understanding the implications of doing and not doing the security procedures. It is also designed to instill good security habits into the minds or consciousness of those who participated in the information society. Good security also requires good co-operation amongst participants.

The OECD guidelines and its implementation are like ivory and ebony. They must lie side by side and keyed creatively to produce a wonderful piece of music. Thus in this case, a suggested implementation plan is included in the referred article for reference or perhaps as a kickoff of a security of information systems and networks campaign. It is also proposed for the actual implementation plan to contain all suggestions so that readers can choose the examples that best suit their circumstances. Now there are already guidelines and the implementation plan, so what’s the next thing is going to be? The answer will most probably be action.