ecrime

The Economic Impacts of Cyber Crime

Newsletter: Opportunities for deterring and fighting cybercrime across non ICT sectors

Number: 7 – October, 2016

The ECRIME consortium partner, University of Lausanne, has produced a report on *Cybercrime Opportunities*, which focusses on opportunities for fighting cyber crime across non-ICT sectors. This report (D7.1) is available for download from the ECRIME website (http://ecrime-project.eu/dissemination/deliverables).

From public awareness to policy makers, a global and schedulable cybersecurity culture should be developed to address all manner of security issues and challenges related to a specific information society. Only an international open and cooperative approach, including international standardization initiatives, could contribute to achieve these universal goals. To put all together the pieces of a global cybersecurity puzzle, answers should be addressed to all kind of actors belonging to political, legal, organizational, technical and social dimension of cybersecurity.

From a political perspective, Governments must understand and develop: the needs for effective cyber diplomacy; an adequate environment to preserve human rights and privacy issues; and identify and organize national and European organizational structures and bodies.

Taking account of the legal dimension and specific needs for justice and police professionals, global understanding of legal issues related to ICT technologies and misuses should be developed. That means the understanding of: computer investigation and forensic methodologies and tools; enhance the level of report of technical incidents; and better define the status of whistle blowers.

Considering business and organization's points of view, executive managers of any size of organisation (including SMEs) should understand basic principles in ICT security management, in particular: assessments of vulnerabilities and threats; defining a security policy; and ensure sustained regulatory compliance and reporting activities.

Security technologies should be: cost effective; user friendly; transparent; auditable; and third party controllable.

Top level European experts from several scientific domains and different industrial sectors are investigating the economic impacts of cyber crime in Europe

The key objectives of **E-CRIME** are:

1. To measure the economic impact of cyber crime on non-ICT sectors
2. To analyse the criminal structures and economies behind such crimes
3. To develop concrete measures to deter such crimes

http://ecrime-project.eu/

FOLLOW US ON

@ECrimeproject

E-CRIME project has received funding from the European Union's Seventh Framework Programme for Security under grant agreement no 607775