



The Economic Impacts of Cyber Crime

Newsletter: European Project E-CRIME

Number: 1 – March 2015

In January 2015 the E-CRIME consortium conducted its first validation workshop in Rome at the offices of Poste Italiane. Attended by over sixty representatives from different industry sectors, cyber security, law and academia, the purpose of this workshop was to bring together a diverse range of experts to discuss the findings produced during the initial stages of this project.

Alongside the work displayed by the E-CRIME consortium, a number of associated cyber crime projects also presented their work to those attending. We have uploaded the slides from these presentations onto the E-CRIME website on the 'Events' page.

Also now available on the website are two Deliverables that have been cleared for public release; found in the 'Dissemination' section. D2.1 covers the development of different taxonomies of cybercrime, and in so doing highlights one of the fundamental problems in this area. That being the lack of common agreement as to what should constitute as 'cyber crime'; i.e. do we restrict it to the offences created within the Council of Europe's Cybercrime Convention, or do we go beyond this to encompass all pre-existing crimes which are now facilitated by computer use? While this question seems academic, without agreed borders over what constitutes cyber crimes we cannot focus effort on effectively tackling them.

D3.1 is a report on how to assess existing cyber crime technologies and best practices. This provides an assessment criteria that is of considerable practical benefits to those within companies or organisations tasked with assessing the potential impact of different anti-cybercrime technologies and best practices either already operating in their organisation, or that they are considering to introduce.

In a fortnight two more deliverables will be upload covering our work on identifying the typical 'journey' (or steps) undertaken by cyber criminals in conducting the most common cyber attacks. By identifying these steps, those tasked with stopping cyber criminals will be better placed to know where they should focus their resources to maximise impact.

Top level European experts from several scientific domains and different industrial sectors have started to investigate 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