



## The Economic Impacts of Cyber Crime

**Newsletter: European Project E-CRIME**

**Number: 2 – May 2015**

**Title: Introducing Deliverable 3.2**

Deliverable 3.2 of the E-CRIME project is a report on the current dominant policies, regulatory and enforcement frameworks, and best practices adopted to counter cybercrime at the European level. This report is available now on the E-CRIME website ([www.ecrime-project.eu](http://www.ecrime-project.eu))

This study maps the existing legislative and enforcement frameworks as relevant to the E-CRIME project. From this mapping exercise one can clearly see that there is fragmentation as regards to legislation, policies and enforcement, as well as regards actors involved in the field of cybercrime. This fragmentation is caused by the very nature of cybercrime, with its disregarding of borders or jurisdictions. As a result, tackling cybercrime requires action and regulation at the local, regional, national and international levels. Following an assessment of the relevant existing legislative and enforcement frameworks Deliverable 3.2 identifies the limitations of the existing system as it is relevant to the E-CRIME project.

By ignoring national borders, the data required to investigate a cybercrime is often found extraterritorially. This requires international cooperation, which may prove difficult in some cases due to differences in both national enforcement legislation and approaches, with national legal frameworks for the investigation of cybercrime in some jurisdictions proving insufficient. Cybercrime also forces law enforcement to rethink their skills due to rapid technological developments. Unfortunately the motivation for prioritising cybercrime varies greatly on national and regional level which further complicates the field.

Security exercises, awareness, training, and information security standards have been highlighted in many key legal and policy documents as being practical solutions for these problems. These best practices can be achieved best through cooperation and information sharing in all areas and on all levels; in particular by specialised cybercrime units. This however, requires commitment by all players involved to act. Moreover, this requires all players involved to know all the other players in the field which might not always be the case due to the fragmentation of actors and sometimes their natural reticence to advertise.

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