BRAIN-be
Belgian Research Action through Interdisciplinary Networks

BCC

Measuring Cost and Impact of Cybercrime in Belgium

DURATION
1/12/2013 - 28/02/2018

BUDGET
684.731 €

PROJECT DESCRIPTION

Background
While offering immense opportunities to the Belgian economy and society, the digital transition has also revealed new threats in the form of cybercrime. The menace can compromise public and national security, transportation, communication, e-commerce, financial, emergency and other services that rely on digital information and infrastructure. Governments need to make informed decisions capable of protecting internet users against cyber threats and promoting economic growth. The exact impact caused by cybercrime is however still unknown. This lack of information has led to uninformed policies and inconsistent assessment of the issue.

Given the far-reaching impact of cybercrime, efficient mitigation measures involve various government sectors in addition to international cooperation. Foreseeing the need for scientific studies in this field, the Federal governmental agreement of 2011 affirmed that relevant stakeholders in combating cybercrime would be consulted. A National Cyber Security Strategy was adopted end 2012, stipulating that any action in this area shall be based on informed decision-making. End 2013 it was decided to create a Belgian Cyber Security Centre (CCSB). Fighting cybercrime is a major challenge and requires policy makers to be well acquainted with the magnitude of the threat. A multidisciplinary research on the cost and impact of cybercrime will support the elaboration and implementation of efficient federal public policies allowing Belgium to take a strategic place on the international scene.

Objective
The project aims to reach an objective, realistic and up to date picture of cybercrime in Belgium and its evolution over time.
A critical assessment of international research reports will be conducted to get an overview on the existing know-how in measuring the cost of cybercrime and the indicators to be used. Supported by the Follow-up Committee, different data sources with information on cybercrime in Belgium will be identified and analysed and an assessment will be made of missing data sources.
Conducted over a period of four years, the research will deliver a better informed and scientifically based view on the menace, thanks to a country-specific model for assessing the impact and cost of cybercrime, to be used in the coming years for collecting comparable and sound information. Moreover, it will also provide strategic insights and guidelines to policy makers on how to advance the implementation of principles integrated in the Belgian National Cyber Security Strategy.

Methodology
The work will be performed in coordination by the different research departments in parallel work packages, under the guidance of the Follow-up Committee.

In WP1, it will be decided in concertation with the Follow-up Committee, what exactly will be the scope of the model to be used to measure cost and impact of cybercrime in Belgium. Track will be kept of publications and sources and the impact they might have on the model the project is developing and implementing in WP2.

Vertical
Three tracks are designed to dig into understanding and monitoring the data on the topic: General public (WP3); Industry (WP4); Public sector (WP5). The research in these three sectors are the vertical pillars on which the model will be designed.

BCC

Horizontal
Supporting this vertical research, an assessment will be made of the investments already made by citizens, industry and government in various countermeasures against cybercrime (WP6). This will provide input not only for measuring cost caused by cybercrime, it will also contribute to the model by providing indicators allowing to predict future costs.

General public
To get a view on the impact of cybercrime on society in Belgium, we will survey the population on their experiences with the internet and cybercrime and how it impacts their behaviour and internet experience. The survey will be executed twice to have a longitudinal research, hence an evolution in the cost and impact can be monitored.

Industry
Concerning the industry sector, data sources with financial losses as a result of online fraud in banking and retail, will be used to seek correlations between losses and certain risk indicators. It will identify candidate technical risk indicators of internet exposure and model the loss based on these indicators for a subset of financial and retail organisations. Track will be kept of changes in the measured risk indicators and the influence they have on possible losses. After validation of the indicators used, these models could be extrapolated to the broader industry sector as a whole. The support of umbrella organisations will be sought for collecting data (survey) within different industry sectors and assessing the model.

Public sector
An analysis will be made of the information and data sources available regarding the public sector and a survey will be conducted, facilitated via the Follow-up Committee and the BelNIS working group, where representatives from different federal entities gather to cooperate and coordinate activities related to Information Security.

Expected research results
Overall, there will be two main research results:

- a methodology and model with proven indicators to be monitored to yield an overview on what is the extent of the cost and impact of cybercrime in Belgium
- an overview of cost and impact of cybercrime in Belgium, obtained by applying the model designed.

CONTACT INFORMATION

Coordinator

Marie-Christine Janssens - Ann Mennens
Katholieke Universiteit Leuven (KU Leuven)
Interdisciplinary Centre for Law and ICT
m-ch.janssens@law.kuleuven.be
ann.mennens@law.kuleuven.be

Partners

Pieter Verdegem
Universiteit Gent (UGent)
Research Group for Media & ICT
pieter.verdegem@ugent.be

Wouter Joosen - Christophe Huygens
Katholieke Universiteit Leuven (KU Leuven)
IMinds-DistriNet Research Group @ KU Leuven
wouter.joosen@cs.kuleuven.be
christophe.huygens@cs.kuleuven.be

Vincent Rijmen
Katholieke Universiteit Leuven (KU Leuven)
COSIC @ KU Leuven
vincent.rijmen@esat.kuleuven.be

LINKS

www.icri.be
www.b-ccentre.be
www.mict.be
https://distrinet.cs.kuleuven.be
http://www.esat.kuleuven.be/cosic/

BELGIAN SCIENCE POLICY OFFICE
Louizalaan 231 Avenue Louise • B-1050 Brussels
Tel. +32 (0)2 238 34 11
http://www.belspo.be/brain-be/ • Email : BRAIN-be@belspo.be

BR/132/A4/BCC