Project No: 607775

Project Acronym: E-CRIME

Project Full Name: Economic Impacts of Cybercrime

Final Report

Period covered: from 01/04/2014 **to** 31/03/2017

Start date of project: 01/04/2014

Project coordinator name:

Version: 1

Date of preparation: 14/04/2017

Date of submission (SESAM): /01/2017

Project coordinator organisation name:
TRILATERAL RESEARCH LTD

Final Report

PROJECT FINAL REPORT

Grant Agreement number:	no 607775
Project acronym:	E-CRIME
Project title:	Economic Impacts of Cybercrime
Funding Scheme:	FP7-Collaborative Project
Project starting date:	01/04/2014
Project end date:	31/03/2017
Name of the scientific representative of the project's coordinator and organisation:	David Wright
Tel:	+44 2075593550
Fax:	
E-mail:	david.wright@trilateralresearch.com
Project website address:	www.ecrime-project.eu

Final Report

Please note that the contents of the Final Report can be found in the attachment.

4.1 Final publishable summary report

Executive Summary

E-CRIME (the economic impacts of cyber crime) is a three year project that started in April 2014 and ended in March 2017. The aim of the project is to reconstruct the spread and development of cyber crime in non-information and communications technology (non-ICT) sectors from the perspective of its economic impact on the key fabrics (i.e., economic and social) and different levels of European society, while also identifying and developing concrete measures to manage and deter cyber crime. E-CRIME aims at paving the way for a gradual shift towards a cyber security thinking that puts increasing resilience, multi-stakeholder co-operation and a comprehensive and integrated approach into the focus of cyber security strategies. In parallel it strives to make a contribution towards the development of comprehensive and economically viable counter-measures supporting the Digital Agenda for Europe, while boosting Europe's economic performance and single market.

E-CRIME focuses on:

1. Mapping the observable developments and effects of cyber crime within and among non-ICT sectors and Member States
2. Assessing existing counter-measures
3. Measuring the economic impact of cyber crime on non ICT-sectors and
4. Developing concrete measures to address cyber crime

E-CRIME does so by adopting an interdisciplinary and multi-level-stakeholder focused approach that fully integrates a wide range of stakeholders' knowledge and insights into the project.

First, the project develops a detailed taxonomy and inventory of cyber crime in non-ICT sectors and analyses cyber criminal structures and economies by combining the best existing data sources with specialist new insights from key stakeholders and experts.

Second, it assesses existing counter-measures against cyber crime in non-ICT sectors in the form of current technology, best practices, policy and enforcement approaches, and awareness and trust initiatives.

Third, having mapped the 'as-is' of cyber crime, the project uses available information and new data to develop a multi-level model to measure the economic impact of cyber crime on non ICT-sectors.

Fourth, it integrates all its previous findings to identify and develop diverse, concrete counter-measures, including enhancement for crime-proofed applications, risk management tools, policy and best practices, and trust and confidence measures.

The final results of E-CRIME are expected to have a positive and durable impact on:

1. *Increasing awareness of policy makers*
2. *Helping business to provide crime-proofed applications*

3. *Increasing the trust and confidence of EU citizens in using cyber applications*

E-CRIME has ten partners from eight European countries.

Figure 1 offers an overview of the various components of the E-CRIME project.

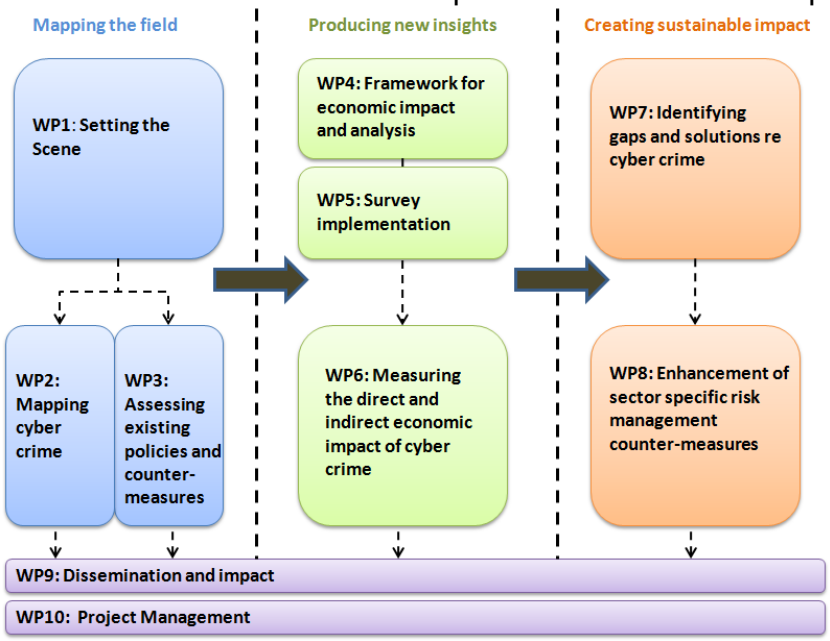

Figure 1: E-CRIME work packages

Website: http://ecrime-project.eu/

Description of main S & T results/foregrounds

The E-CRIME project met all of its stated objectives through the course of the project. The table below details the initial 7 objectives and the degree of achievement towards them.

#	Initial Objectives	Degree of achievement	Measurable & verifiable
1	Create a taxonomy and an inventory on crime committed against non-ICT sectors through the use of communication networks.	A taxonomy/inventory has been developed with the help of the ESF, data collection and further desktop research. WP2 will develop taxonomy and an inventory of cyber-crime in non-ICT sectors.	1) Deliverables from WP1 and WP2. 2) Publications
2	Analyse the criminal structures and economies behind such crimes.	Detailed criminal journeys have been developed from a perpetrators and victim viewpoint. These journeys have been used as the basis to develop the attack scripts and manual as part of the cybersecurity awareness programme.	1) Deliverables from WP2 2) Exploitation output from WP9, including training programme and manual 3) Publications 4) Scripts have been shred with major UK Banks and included in their training programme 5) Presentation in conferences /meetings

3	Measure and analyse the economic impact of cyber-crime on non-ICT sectors (e.g., transport, energy, finance, health, etc.).	An economic model has been developed and has supported the creation of practical tools for exploitation in WP8: risk management tools (e.g., a cost-benefit decision tool for cybersecurity investments and a data-driven tool to identity best actions to respond to fraud in the financial sector)	1. Deliverables from WP4, 5 &6 2. Publications 3. Presentation in conferences and meetings 4. Development of tools in WP8
4	Develop concrete measures and methods to deter cybercrime	A list of common opportunities has been identified and practical solutions developed. This includes: the development of risk management tools, including a data-driven tool to identity best actions to respond to fraud in the financial sector and a cost benefit model to support investment decision on countermeasures, recommendation for regulatory interventions including policy impact assessment sector by sector, a guide for best practices sector by sector, guidance and requirements for developing improved crime proofed applications and a high level roadmap supporting the	1. Deliverables from WP7 & WP8 2. Publications 3. Presentations in conferences and meetings
5	Present effective measures for the management of risks related to cyber-crime and help businesses to provide crime-proofed applications.	Specifically, E-CRIME has developed risk management tools, including an holistic data-driven approach to risk identification to fraud in the financial sector and a cost benefit model to support investment decision on countermeasures, and sector specific guidance and	1. Deliverables from WP8.
6	Increase the trust and confidence of EU citizens in using cyber applications.	The consortium work together with a leading bank to develop a data-driven holistic approach to risk quantification to respond to fraud in the financial sector and e-commerce sector. This tool takes in consideration risk of on-line avoidance as result of cybercrime and how to increase trust with end-users. We have also developed guidelines and recommendations on how to	1. Deliverables from WP5 & & WP8 2. Publications 3. Presentations in conferences and meetings

7	Increase the awareness of policy- makers, and foster the understanding and the awareness of the non-ICT sectors	Several activities were carried out to support this objective. This includes: developed a training awareness programme, including a manual, the organisation and running of a training event, the dissemination of several policies briefs, the running of validation workshops, liaison and newsletters for the ESF, participation in conferences and external events.	1 Workshops for WP2&3, WP5 , WP7 2. Final conference from WP 9 3. Deliverables from WP9 4. Presentations in meetings and conferences

Specifically ,

WP1: Setting the scene. The E-CRIME team has developed the project handbook, which will be used by the partners as a navigation guide during the development of the project. The team has also developed an extensive contact list of stakeholders and provided an in-depth analysis of their motivations, while setting up the E-CRIME Stakeholder Forum (ESF), comprising 90 members including associated ones. The ESF has supported the working of the project across the three-year plan. Finally, the consortium has agreed a selection methodology and finalised the selection of which representative non-ICT sectors and Member States the project will focuses on.

WP2: Mapping Cybercrime. Objectives for WP2 were to: (1) investigate definitions of cyber crime and provide a conceptual framework and categorisation of cyber crime in non-ICT sectors to be used for the project: (2) develop an inventory of crime committed against non-ICT sectors through the use of communication networks; (3) analyse the structures of cyber crime networks, their interactions and the economies and criminal revenue streams that support these networks; and (4) develop perpetrator and victim "journeys".

WP3: Assessing existing policies and counter-measures. The objective has been to identify, assess and monitor existing and new counter-measures in the field of regulation, enforcement, technologies and industry best practices. The consortium submitted the report for Task 3.1 titled "Anti-Cybercrime technologies and best practices assessment and monitoring." The report proposes a set of criteria to assess such anti-cybercrime technologies and industry best practices, which are flexible enough to be adopted for various Non-ICT sector types and all sizes of organisations. A key aspect to this was ensuring that the approaches could be adapted by a wide range of industries and categorisation of crimes. Within the work for this task a desktop analysis of several representative examples of existing anti-cybercrime technologies and best practices were researched and presented. Using a mix of case studies and cyber range replication in a controlled environment, a selection of criminal journeys from WP2 (D2.3) have been explored in order to derive evaluation insights on the selected anti-cybercrime technologies and best practices. The objective of this work is to both define the criteria for the assessment of existing cybercrime practices and anti-cybercrime technologies and best practices and assess the selected anti-cybercrime technologies and best practices via case studies. It assesses the effectiveness of these counter-measures for preventing, deterring and managing cybercrime and includes the on-going monitoring of

these counter-measures through the lifespan of the project with a specific focus on non-ICT sectors and will take into consideration relevant output from future Work Packages.

D3.2 assesses the dominant policies, regulatory and enforcement frameworks and best practices concerning cybercrime relevant for the E-CRIME project, taking into account the economic impact on the non-ICT sector, the most relevant threats to the non-ICT sector (WP2) and countermeasures (D3.1) and by focusing on the Council of Europe Cybercrime Convention and EU legal frameworks. D3.2 shows that cyber incidents relevant for the economic impact on the non-ICT sector fall within the categories of cybercrime in the Convention. These cyber incidents in many cases may be prevented before they occur by solid Network and Information Security, meaning by applying countermeasures including best practices and policies as well as technological countermeasures. Not all cyber incidents may be prevented. For those incidents that cannot be prevented, an effective enforcement framework including the necessary investigative powers and procedures, mutual assistance, international cooperation, etc. is necessary in order to combat cybercrime. On a European level, there is a framework regulating cybercrime in place. The Convention is the legal framework of reference and is supported by various EU documents. There are however still a number of limitations or gaps in this framework which have been identified in D3.2 by studying the relevant policies, legislative frameworks and enforcement activities.

WP4 Framework for economic impact and analysis: The higher-level objective of work package 4 is the collection of empirical data for an impact assessment of cyber-crime on non-ICT sectors. We developed a framework of hypotheses and collected data on the views of EU citizens' and industry stakeholders via a telephone survey and face-to-face expert interviews. The results of the industry interviews and the consumer survey are documented in the form of an executive summary, a policy brief and detailed appendixes in deliverable D4.2. Highlights have also been presented at the validation workshop in The Hague (Jan. 25/26. 2016). Lastly, the empirical findings in WP4 also informed and validated the economic model, which was developed in WP6.
One conference paper has been written and presented at the Workshop on the Economics of Information Security (WEIS) 2014, in State College, USA by P4WWU[1]. Based on this early work one journal article has been submitted by P11UIBK and has been accepted for publication by the IEEE journal: Transactions on Dependable and Secure Computing (TDSC).[2] The article "Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance" analyses consumer reactions to perceived risk of cyber crime in Europe. Existing behavioral models to model decisions of online service usage are integrated and augmented to include perceived risk of cyber crime. The resulting model is using a secondary analysis of a pan-European survey. The article is particularly relevant for the E-CRIME project, as the behavioral models, used in the article, largely informed the consumer survey (D4.1).
A second conference paper has been accepted at the Workshop on the Economics of Information Security (WEIS) 2016, in Berkeley, USA. The paper "*Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries*" has been jointly written by UIBK and TUD. It analyses the costs of consumer-facing cybercrime based on the data collected in the ECRIME consumer survey.
The results of the industry interviews and the consumer survey have been presented to

[1] Riek, M., Böhme, R., and Moore, T. (2014). "Understanding the Influence of Cybercrime Risk on the E-Service Adoption of European Internet Users." In Proceedings of the 13th Workshop on the Economics of Information Security (WEIS), Pennsylvania State University, State College, Pennsylvania.
[2] Riek, M., Böhme, R., and Moore, T., "Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance," *IEEE Transactions on Dependable and Secure Computing*, vol.PP, no.99, pp.1,1, doi: 10.1109/TDSC.2015.2410795

and discussed with industry stakeholders at the second ECRIME validation workshop in The Hague, Netherlands. Furthermore, they have been presented at the TRESPASS 2016 WINTER SCHOOL ON SECURITY IN SOCIAL-TECHNICAL SYSTEMS[3] in January 2016 and at the BIGS Capacity Building Workshop on "Economics of Cybersecurity: Cost-benefit considerations, Incentives and Business Models"[4] in April 2016.

WP5 Survey Implementation This work package focused on collecting survey data in six selected Member States. The aim was to carry out a survey on the impact of cybercrime on non-ICT sectors. The survey was conducted using the questionnaire designed as part of WP4. The data collected is used in WP6, to calibrate the economic models.
The survey set up has started in June 2015, once the questionnaire was finalised (as part of work package 4). The survey was implemented in six countries: Estonia, Germany, Italy, the Netherlands, Poland and the UK, through telephone interviews.
The aim was to collect information from internet users in each country. The sampling approach was based on quotas on age, gender and region, representative of the online population in each country.
The main deliverable – D5.1 survey dataset – was provided in November 2015 (unweighted) and December 2015 (weighted). The data was provided in SPSS format.
A total of 6394 interviews were conducted across the six countries. The following table presents the number of interviews carried out in each country:

Number of interviews	
Country	**Total**
Germany	1150
Estonia	1058
Italy	1064
The Netherlands	1032
Poland	1038
The UK	1052
Total	6394

Apart from the main deliverable (D5.1 - final SPSS dataset), the following outputs were produced:

- Interim dataset (with preliminary results, prior to closing fieldwork)
- Excel spreadsheets presenting the aggregated results for each question
- A technical report describing the survey methodology.

The survey results were analysed by UIBK (and presented in deliverable D4.2) and also informed the economic model (presented by TUD in deliverable D6.2).

WP6 Measuring the direct and indirect economic impact of cyber crime. In WP6 we developed, calibrated and validated a multi-layer model to measure the economic impact of cyber crime on the selected non-ICT sector. As part of the validation, we held a workshop in den Haag with stakeholders from all the relevant non-ICT sectors. Prior to

[3] https://www.utwente.nl/ctit/archive/!/2015/10/334989/trespass-2016-winter-school-on-security-in-social-technical-systems
[4] http://www.bigs-potsdam.org/index.php/en/events/current-events

the development of the model, during Task 6.1 and Task 6.2, we argued that estimating the costs of cybercrime is a valuable, and indeed irreplaceable, tool for policy makers and the criminal justice system. However, while the concept of monetizing the impact of cybercrime for many people seems feasible, and maybe even reasonable, such calculations have many disadvantages and generate estimates that are from reality. From the analysis based on the state-of-the-art we identified the drawbacks of current cybercrime studies and described the challenges that have to be addressed before generating cost estimates. Moreover, we have analysed existing data sources depending on the measurement methodology and how different aggregation models have leveraged these data to generate unrealistic costs estimates. Due to the misuse and limitations of existing data sources, the true burden of cybercrime on human society still remains unknown.

To fulfil this information gap, in D6.1 we presented a set of basic economic foundations that serve as basis for our model. We split the cost of cybercrime into different levels: cost of cybercrime to individual agents and cost of cybercrime to society.
In D6.2 and D6.3, we presented: (i) a qualitative assessment of the economic impact of cybercrime on non-ICT sectors based on the model developed in Task 6.2; (ii) a quantitative assessment of the key economic impacts of cybercrime on non-ICT sectors with the data collected through WP4 and 5 and the suitable external data sources as assessed in Task 6.1; and (iii) a comparison of the economic impact of cybercrime across the selected non-ICT sectors. Finally, we concluded that the five non-ICT sectors analysed in this project suffer from cybercrime but to different degrees. The economic impact of cybercrime varies by industry segment, where financial services and energy companies experience higher impact than entities in retail, transport and health care sectors. Moreover, the short-term economic impact is not distributed uniformly across the different categories. Some sectors like financial services and retail have costs across all three categories while other sectors like health care mainly have anticipation costs.
Finally, we validated the qualitative and quantitative assessment in a workshop hosted in January 2016, The Hague. With over 40 stakeholders from the different non-ICT sectors, the results were validated and the feedback incorporate in D6.3.

WP7 Identifying gaps and solutions re cybercrime. The main objective of this work package is to integrate, combine and compare results from previous work packages (WPs 2, 3, 4, 5 & 6), identifying opportunities for deterring and managing cyber crime, including technology, regulation, co-ordination, risk management, and awareness and trust initiatives. These opportunities were validated with stakeholders.

General opportunities to fight cyber crime were identified in D7.1 and validated with a group of stakeholders in Lausanne (M13 and D7.2). Opportunities maps were developed as part of D7.1, which drove and informed the work of WP8. The maps provided the initial perimeter where specific opportunities were selected for development in WP8.

The map identified main high level recommendations within a comprehensive framework. Opportunities were discussed within the awareness/cultural, political, legal, organisational and technical dimensions. D7.1 was based on the state of the art of knowledge on cyber crime. The practical experience of operational stakeholders in the fight against cybercrime and cybersecurity professionals within companies has also been taken into consideration to build those perspectives. The recommendations, seen as an opportunity, seek to remain directly enforceable.

The added value of the opportunity maps come from the consistency of their implementation based on a trans-disciplinary, trans sectorial and integrative

understanding. Fighting against cybercrime could not succeed without a strong implication at all political levels. This is turn implies that only solutions combining the efforts of public and private sectors, also including citizens, can succeed. We validated the findings of WP7 and the opportunity maps in a workshop in Lausanne, held in May 2016. We reached our core objective by engaging stakeholders, decision makers and researchers around the key findings of the report and the opportunities and recommendations.

The opportunities were also developed, socialised and presented at different venues and forums such as, Lausanne, Financial cyber crime conference (4 Dec 2015), New Delhi, Cyber weapons and cyber power (2 Feb 2016), New Delhi, Is digital privacy and personal safety compatible (3 Feb 2016) and Université Savoie Mont Blanc, France Journée nationale du réserviste – Conférence: Cyber-menaces à l'horizon 2020: enjeux, anticipation et resilience (22 March 2016).

WP8 Enhancement of sector specific risk management counter. The main objective of this work package is to develop sector-specific methods, tools and measures to fight cyber crime.

In Task 8.1 we developed sector-specific methods, tools and risk management frameworks to manage cyber crime risk in the selected non-ICT sectors. This was based from the economic impact model in WP5, findings from WP6 and desk-top analysis of state-of-the- art work on cyber crime risk management. We undertook a survey with PLUSCARD to examine payment card fraud in the financial and retail sector within Germany, building on the results of the citizen survey undertaken in WP5. After discussing the problem during the E-CRIME industry interviews, PLUSCARD, a German payment card processor and stakeholder in the E-CRIME stakeholder forum, offered us the incredible opportunity to collaborate for a behavioral study of their customers, in particular the victims of payment card fraud. UIBK conducted a controlled experiment with approx. 900 participants to measure the victims' perception of incidents and their reactions after victimisation. Resources for this additional study were approved by the Project Officer. Data collection commenced in M32. Output of this work provided a thorough estimation of the economic impact of payment card fraud to be utilised as the foundation for data-driven cyber risk management tool. The team in TUD led the production of the sector-specific risk management sections and production of the overall risk framework sector by sector. Based on the output of Task 8.1, *D8.1 – Executive summary and brief: Sector-specific cyber crime risk management including detailed appendixes on sector specific cyber crime risk management* were produced

In Task 8.2 the team applied the opportunities identified in WP6 and findings from WP2 and WP3, to draw up an initial list of business and technological requirements for sector-specific applications in the selected non-ICT sectors. The final requirements provide practical, sector guidance on crime-proofed application advancements, including identification of key functionalities, and other technological counter-measures for the selected non-ICT sector. We also develop guidance on how sector-specific, crime-proofed applications can be developed, tested, assessed and integrated into existing IT infrastructures and business processes.

In addition, 10+ attack scenarios across the sectors and included potential countermeasures to address the attacks were developed. Then we conducted cost-calculation methodology for the countermeasures listed, before indexing the countermeasure and the related cost inside an International framework for cyber security. In this case, the framework is the National Cyber Security Framework of NIST that is the easier to adopt for SMEs. Aimed at Public and Private stakeholders, Large and Small and Medium Enterprise, the developed cost calculation methodology is helpful to present

the level of annual cost of information security countermeasures to the top manager of the entities that decide to adopt it. Since the framework in which the expenditures is inserted is an International one, it is very easy to be approached also from stakeholder with a low level of Information Security competencies
The output from Task 8.2 is *D8.2 – Report: Sector specific crime-proofed applications and other technological counter-measures.*

In Task 8.3 we built from the opportunities in WP6 and the counter-measure assessment in WP3 to identify if new legal and policy measures, as well as new responses, should be adopted at Member States and European level to deter and manage cyber crime in each of the selected non-ICT sectors. Our regulatory innovation focused on developing institutional mechanisms and tools that allow transnational enforcement, support co-operation across European Member States, and beyond, as well as enhance co-ordination and interoperability among different stakeholders.
The output from Task 8.3 is *D8.3 – Report: Recommendation for regulatory innovation and measures*.

In Task 8.4 we focused on enhancing and developing sector-specific industry best practices in deterring cyber crime in each of the selected non-ICT sectors. The consortium utilised the output from WPs 6 and 7 and employed their cyber range to test the efficacy of counter measures. They also took into account the regulatory measures developed from Task 8.3 with interactive sessions conducted as part of the new training workshop of industry and law enforcement representatives planned for M35. This workshop included cyber law enforcement representatives from MS across Europe, as well as Interpol and Europol reps and selected member of ESF drawn from law enforcement.

The Deliverable from this Task is *D8.4 – Report: Sector-specific enhancements in industry best practices*.

In Task 8.5 we have identified sector-specific initiatives across Member States and beyond relating to building awareness, trust and confidence in the selected non-ICT sectors. The partners developed sector-specific recommendations and guidelines at different levels (individual, company, state, civil society, EU) to increase awareness, trust and confidence among end users in the selected non-ICT sectors. We identified actors and stakeholders best suited to implement these sector-specific guidelines and recommendations. This encompasses a broad range of potential actors (e.g., states and industry players to telecommunications operators, ISPs, police, etc.).
This task produced *D8.5 – Report on high level roadmap and implementation plans for sector-specific counter-measures.*

In Task 8.6 the consortium organised and presented the final findings of the project in a final conference organised in London and produced a final executive summary of the project, Final report (D8.6) including high level roadmaps and implementation plans for the solution put forward in the previous reports.

Through Work package 9 (WP9) partners had particular success in disseminating the results of the E-CRIME project to target stakeholder groups, with the E-CRIME stakeholder forum list boasting 90 members including associate. The E-CRIME project is represented by an engaging and active website, the publication of press releases/newsletters, its social media accounts (Twitter, LinkedIn), by attendance at 3rd party events, E-CRIME events, including the training awareness day, and a number of publications in peer reviewed journals. Novel dissemination techniques were also

employed, such as disseminating training manual with project deliverables. As a result, E-CRIME was mentioned in a number of 3rd party newsletters and websites.

Potential impact and main dissemination activities and exploitation results

The E-CRIME impact falls along the following main categories: methodological / empirical impact; knowledge sharing impact, including increasing co-ordination and knowledge sharing among key cyber security stakeholders; policy impact; awareness; industry oriented results and/or impact, including helping business to provide crime-proofed applications; economic/ competitiveness impact; strategic impact and societal impact including increasing the trust and confidence of EU citizens in using cyber applications and other wider societal implications. The table below details the exploitation activities and outputs produced during the project, provides a brief description of the activities/outputs together with its end-user focus and identifies for each activity and the main impact produced.

Exploitation activities/output	General Approach & End-Users	Impact
Guidelines describing how to use the attack scripts in a cybersecurity awareness training programme. These guidelines were included into a final training manual.	Developing and writing down concrete steps (illustrated with examples) how to use developed attack scripts as a part of a cybersecurity awareness training programme. Relevant for any institution belonging to one of our five focus categories (transport, retail, finance, healthcare, energy).	• **Awareness impact**: Increase awareness of policy makers and key industry and stakeholder • **Industry impact:** support industry in developing crime-proofed applications • **Economic/ competitiveness: impact:** increase the competitiveness of European industry players including security providers • **Societal impact**: increasing the awareness of citizens and society as a whole in relation to cyber crime
Data-Sets & Interview-Schedule from consumer survey deposited for future use.	The data sets from the victim survey has been deposited in one or more publicly accessible repositories, situated within the EU, at the end of the project. The data sets from the trans-Europe telephone survey constitute a resource for future analyses, both as a single study and as part of meta-studies. They also constitute a time-stamped sample of opinions and levels of economic cyber crime. The survey schedule provides a standardised set of questions enabling re-sampling within longitudinal studies – this assists in measuring changes in opinions and cyber crime levels/impacts over time. Academics and statisticians are the anticipated end-users.	• **Empirical/methodological impact**: this is both empirical and methodological since the central empirical result of E-CRIME will provide an empirical benchmarking and methodological toolkit for end-users. • **Societal impact**: this helps the overall development of empirical methodology to assess the impact of cybercrime

Crime Scripts for different cyber-criminal journeys . These scripts were included into a final training manual.	The criminal journeys, depicting the identified steps an attacker must complete when undertaking different types of cyber attacks provide an invaluable tool with two primary anticipated benefits. Firstly it provides a clear graphic visualisation of the processes and steps that constitute what are often complex cyber attacks. Secondly, by layering multiple scripts on top of each other, and/or by focussing on the most prolific types of cyber crimes, one can better identify the 'pinch-points' for disrupting future attacks. End-users here include industry (both the targets of cyber crime as well as those developing cybercrime mitigation technologies), and law enforcement agencies.	• **Awareness impact**: Increase awareness of policy makers and key industry and stakeholder • **Industry impact:** support industry in developing crime-proofed applications • **Economic/ competitiveness: impact:** increase the competitiveness of European industry players including security providers • **Societal impact**: increasing the awareness of citizens and society as a whole in relation to cyber crime
Awareness Training Program and manual including and the organisation of a training event	Targeted at Cyber Crime LEA units in Europe, where we validate and provide this material to them so they can use it for three purposes: A - Validate its efficacy for their own internal training program for new officers and trainees B- Provide them the work as a training manual in order to allow them to become champions and disseminate further C- Allow them to be able to communicate this work to industry as part of their Protect and Prevent strategies	• **Awareness impact**: Increase awareness of policy makers and key industry and stakeholder • **Industry impact:** support industry in developing crime-proofed applications • **Knowledge sharing impact**: knowledge sharing across among relevant stakeholders • **Societal impact:** support a knowledge sharing culture within Europe
The development of an holistic approach to risk quantification to respond to fraud in the financial sector	The additional survey were used as the basis for developing a data drive approach on the impact of online fraud in the financial sector measuring the impact of cyber crime for online e-commerce as the result of avoidance activities while supporting the identification of the best action to respond to the fraud. This is relevant to the financial sector operators, specifically banks.	• **Industry impact:** support industry in developing crime-proofed applications • **Economic/ competitiveness: impact:** increase efficiency and the competitiveness of European industry players including security providers • **Societal impact:** increasing the trust and confidence of EU citizens in using cyber applications
The development of a practical cost/ benefit tool/model to support investment decisions on countermeasures	A framework with a cost/benefit calculation methodology and guideline able to monitor the total amount of the expenditures in Information Security, divided in categories and that also represents a	• **Industry impact**: support industry in managing cyber crime risk • **Economic/ competitiveness: impact:** increase efficiency and the competitiveness of

	method to understand a cost/benefit of each countermeasure put in place. The result is a list of countermeasures with a cost calculation methodology, inserted in an easy international framework. The industry player in general would be able to understand in that way how much they spend on information security activities and would be also able to identify the percentage of expenditures between the categories. This applicable across all the E-CRIME sectors. It aimed at Public and Private stakeholders, Large and Small and Medium Enterprise. The cost calculation methodology helps present the level of annual cost of information security countermeasures to the top manager of the entities that decide to adopt it. The framework in which the expenditures will be inserted is an International one, very easy to be approached also from stakeholder with a low level of Information Security competencies.	European industry players including security providers • **Societal impact**: Indirectly by effectively supporting companies in managing cyber crime risk this will increase the trust and confidence of EU citizens in using cyber applications
A guide for best pratices sector by sector	A practical guide to help industry users to identify/use best pratices in their sector . This is for all the E-CRIME sectors.	• **Industry impact**: support industry in managing cyber crime risk • **Economic/competitiveness impact:** increase efficiency and the competitiveness of European industry players including security providers • **Societal impact** : Indirectly by effectively supporting companies in managing cyber crime risk this will increase the trust and confidence of EU citizens in using cyber applications • **Strategic impact**: it will have strategic impacts for the European Union, particularly in relation the development of Digital Single Market and in support of the Digital Single Strategy as well as the European cyber security strategy
A guidance and requirements for cyber crime management and	This is a guide, sector by sector, summarising the key requirements and guidelines to managing cyber	• **Industry impact:** support industry in developing crime-proofed applications

mitigation	crime and mitigate its risk/impact. Industry players in all the E-CRIME sector are the key beneficiary.	• **Economic/competitiveness impact:** increase efficiency and the competitiveness of European industry players including security providers • **Societal impact**: Indirectly by effectively supporting companies in managing cyber crime risk this will increase the trust and confidence of EU citizens in using cyber applications
Recommendation for regulatory interventions including policy impact assessment sector by sector	This is targeted to policy makers to support their regulatory and policy interventions and actions to improve cyber security in Europe	• **Awareness impact**: Increase awareness of policy makers • **Policy impact:** support policy makers in developing new intervention to improve cyber security in Europe • **Societal impact:** create a suitable regulatory and policy environment and culture at the European level • **Strategic impact**: it will have strategic impacts for the European Union, particularly in relation the development of Digital Single Market and in support of the Digital Single Strategy as well as the European cyber security strategy

Address of project public website and relevant contact details

Project website: http://ecrime-project.eu
Twitter: https://twitter.com/ECrimeproject
LinkedIn: https://www.linkedin.com/in/ecrime-project-

4.2 Section A (public) Publications

LIST OF SCIENTIFIC PUBLICATIONS, STARTING WITH THE MOST IMPORTANT ONES										
No.	Title / DOI	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Date of publication	Relevant pages	Is open access provided to this publication ?	T
1	Utilising Journey Mapping and Crime Scripting to Combat Cybercrime and Cyber Warfare Attacks	Tiia Sõmer, Bil Hallaq, Tim Watson	Journal of Information Warfare	Vol. 15, Issue 4	Mindsystems Pty. Ltd. ISSN 1445-3312	Yorktown, Virginia: United States	31/12/2016	39-49	No	P revi
2	A multi-level approach to understanding the impact of cyber crime on the financial sector 10.1016/j.cose.2014.05.006	Lagazio, Monica, Nazneen Sherif, and Mike Cushman	Computers & Security	Vol. 45	Elsevier Ltd		September 2014	58-74	No	P revi
3	Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance 10.1109/TDSC.2015.2410795	Markus Riek, Rainer Böhme, Tyler Moore	IEEE Transactions on Dependable and Secure Computing	Vol. 13, No. 2	Institute of Electrical and Electronic Engineers ISSN 1545-5971	United States	01/03/2016	261-273	No	P revi
4	Understanding the Influence of Cybercrime Risk on the E-Service Adoption of European Internet Users	Markus Riek, Rainer Böhme, Tyler Moore	13th Workshop on the Economics of Information Security (WEIS)	NA			2014		Yes	Wo pa
5	Is the Cost of Cybercrime Elusive?	Bil Hallaq, Monica Lagazio, Timothy Mitchener-Nissen	CyberTalk Magazine	Issue 7	Soft Box Ltd	York, United Kingdom	2015	60-62	Yes	Ar
6	Cyber criminal journeys to support forensic investigation and response deployment	Monica Lagazio, Timothy Mitchener-Nissen, Tiia Sõmer and Bil Hallaq	Digital Forensics Magazine	Issue 23	TR Media	United Kingdom	April 2015		No	Ar

7	Understanding the Victim Journeys and Victim Costs of Cybercrime	Monica Lagazio, Timothy Mitchener-Nissen, Tiia Sõmer and Bil Hallaq	Digital Forensics Magazine	Issue 25	TR Media	United Kingdom	November 2015		No	Art
8	Utilising Journey Mapping and Crime Scripting to Combat Cyber Crime	Tiia Sõmer, Bil Hallaq, Tim Watson	ECCWS conference proceedings		Academic Conferences and Publishing International Limited ISSN 2048-8602	United Kingdom	2016	276-281	No	P revi

LIST OF DISSEMINATION ACTIVITIES								
No.	Type of activities	Main Leader	Title	Date	Place	Type of audience	Size of audience	Countries addressed
1	Oral presentation to a scientific event	UNIVERISTY OF LAUSANNE	Les impacts économiques du cybercrime	07/11/2014	Lausanne, Switzerland	Industry – LEA	70	European audience
2	Oral presentation to a scientific event	UNIVERISTY OF LAUSANNE	Impacts économiques de la cybercriminalité	04/12/2015	Lausanne, Switzerland	Scientific community (higher education, Research) – Industry - Government	120	European audience
3	Oral presentation to a scientific event	UNIVERISTY OF LAUSANNE	Forum International de la Cybersécurité	25/01/2016	Lille, France	Scientific community (higher education, Research) - LEA	70	European audience
4	Oral presentation to a workshop	UNIVERISTY OF LAUSANNE	Presentation and discussion at the Observer Research Foundation	02/02/2016	New Delhi, India	Scientific community (higher education, Research)	45	International audience
5	Oral presentation to a workshop	UNIVERISTY OF LAUSANNE	Presentation and discussion at the Indian Institute of Technology (Centre of Excellence in Cyber Systems and Information Assurance)	03/02/2016	New Delhi, India	Scientific community (higher education, Research) - Policy makers	25	International audience
6	Oral presentation to a scientific event	UNIVERISTY OF LAUSANNE	Conférence francophone sur le renforcement de la cybersécurité et de la cyberdéfense	09/02/2016	Grand Bassam, Ivory Coast	Scientific community (higher education, Research) – Government - LEA	80	International audience
7	Oral presentation to a scientific event	UNIVERSITY OF WARWICK	European Information Security Summit	10/02/2015	London, UK	Industry – Government - LEA	400	European audience

8	Oral presentation to a Law Enforcement Event	UNIVERSITY OF WARWICK	Inaugural National Cyber Crime Conference (NCA)	14/10/2014	Nottingham, UK	LEA - Government	100	United Kingdom
9	Oral presentation to a Law Enforcement Event	UNIVERSITY OF WARWICK	Forensics Europe Expo	20/04/2016	London, UK	LEA – Government - Industry	150	International audience
10	Oral presentation to a scientific event	TRILATERAL RESEARCH LTD & UNIVERSITY OF WARWICK	ARES Conference on Availability, Reliability and Security – Is measuring cybercrime illusive?	31/08/2016	Salzburg, UK	Scientific community (higher education, Research) - Civil society - Policy makers	350	International audience
11	Oral presentation to a scientific event	TRILATERAL RESEARCH LTD & UNIVERSITY OF WARWICK	World eID Conference	28/09/2016	Marseilles, France	Scientific community (higher education, Research) - Policy makers	350	International audience
12	Participation in networking event	UNIVERSITY OF GRONINGEN	Global Conference on Cyberspace	16-17/04/2015	The Hague, Netherlands	Government – Scientific Community – NGOs - Industry	1000	International audience
13	Oral presentation to a scientific event	UNIVERSITY OF GRONINGEN	e-Justice and e-Law Conference	13-14/10/2014	Rome, Italy	Government - LEA	150	European audience
14	Oral presentation to a workshop	UNIVERSIT OF GRONINGEN & UNIVERSITY OF INNSBRUCK	The Workshop on the Economics of Information Security (WEIS)	12/06/2016	San Francisco, USA	Scientific community (higher education, Research) - Policy makers	50	International audience
15	Oral presentation to a workshop	UNIVERSITY OF INNSBRUCK	4th Workshop on Bitcoin and Blockchain Research; Financial Cryptography and Data Security 2017	03-07/04/2017	Malta	Scientific community (higher education, Research) - Industry	50	International audience
16	Oral presentation to a workshop	UNIVERSITY OF INNSBRUCK	Moderne Kriminalität - der schlaue Kriminelle agiert von zu Hause	10/03/2017	Bonn, Germany	Judiciary	45	

17	Participation in networking event	INTERPOL	Conference on Article 15 safeguards and criminal justice access to data	19-20/06/2014	Strasbourg, France	Public and Private sector institutions – LEA	100	European audience
18	Participation in networking event	INTERPOL	World Innovation Conference Law Enforcement Information Management – WICLEIM 2014	10-12/06/2014	Amsterdam, Netherlands	LEA	250	International audience
19	Oral presentation to a conference	INTERPOL	22nd INTERPOL Asian Regional Conference	15-17/04/2015	Singapore	LEA	160	International audience
20	Participation in networking event	INTERPOL	11th Heads of National Central Bureaus (NCB) Conference	24-26/03/2015	Lyon, France	LEA	265	International audience
21	Oral presentation to a conference	INTERPOL	43rd European Regional Conference	19-21/05/2015	Bucharest, Bulgaria	LEA	150	International audience
22	Participation in networking event	INTERPOL	Octopus2015 Conference on Cooperation against Cybercrime	17-19/06/2015	Strasbourg, France	LEA	300	International audience
23	Hosted a stand at this event	INTERPOL	INTERPOL Heads of National Central Bureau (NCBs) conference	07/03/2017	Lyon, France	LEA	300+	International audience
24	Oral presentation to a workshop	INTERPOL	1st INTERPOL digital forensics expert group meeting	21/06/2016	Madrid, Spain	LEA	40	European audience
25	Oral presentation to a conference	GCSEC	Cyber Security Incident Handling: use case	16/07/2014	Rome, Italy	LEA - Government representatives - Industry	100	European audience
26	Oral presentation at a conference	GCSEC	Cyber Defence Symposium	14/052015	Rome, Italy	Scientific community (higher education, Research) - Policy makers - LEA	100	European audience

27	Oral presentation at a workshop	GCSEC	Attacco Cyber: esperienze operative per la resilienza del business	15/06/2016	Rome, Italy	Scientific community (higher education, Research) - Policy makers – Industry	35	European audience
28	Networking at a conference	GCSEC	Dream It - Westcon	07/07/2017	Rome, Italy	Industry	100	European audience
29	Networking at a conference	GCSEC	Cyber Security Congress Information security: fail often in order to succeed	14-16/09/2016	Sibiu, Romania	Scientific community (higher education, Research) - Policy makers – Industry	150	European audience
30	Oral presentation at a workshop	GCSEC	ATM: A look at the future and emerging security threats landscape	22/09/2016	Rome, Italy	Banking sector – LEA- Research community	50	International audience
31	Oral presentation at a summit	GCSEC	Global Cyber Security Summit	31/10-01/11/2016	Rome, Italy	Scientific community (higher education, Research) - Policy makers – Industry	200	International audience
32	Oral presentation at a workshop	GCSEC	Advanced Persistent Threats: real cases	22/11/2016	Rome, Italy	Industry – Policy makers - Cybersecurity	25	National audience
33	Oral presentation in a summit	GCSEC	Cloud Access Security Broker	15/12/2016	Rome, Italy	Industry	50	International audience
34	Oral presentation at a workshop	TECHNISCHE UNIVERSITEIT DELFT	Assessing ICT Security Risks in Socio-Technical Systems	13-16/11/2016	Germany	Scientific community (higher education, Research) - Policy makers – Industry	20	European audience
35	Oral presentation at a workshop	TECHNISCHE UNIVERSITEIT DELFT	Keynote and workshop for the Ministry of Economic Affairs on "Economics of Cybersecurity"	17/10/2016	The Hague, Netherlands	Scientific community (higher education, Research) - Policy makers	30	National audience

36	Oral presentation at a workshop	TECHNISCHE UNIVERSITEIT DELFT	The Value of Cyber Risk Quantification	13/10/2016	Amsterdam, Netherlands	LEA – Policy makers	18	National audience
37	Oral presentation at a meeting	TECHNISCHE UNIVERSITEIT DELFT	Framework for cyber risk assessment	23/06/2016	The Hague, Netherlands	LEA – Policy makers	25	National audience
38	Oral presentation at a conference	TALLINNA TECHNIKAULI KOOL	2nd Interdisciplinary Cyber Research (ICR) workshop 2016	02/07/2016	Tallinn, Estonia	Scientific community (higher education, Research) - Policy makers – Industry	70	International audience
39	Oral presentation at a conference	TALLINNA TECHNIKAULI KOOL	15th European Conference on Cyber Warfare and Security	07-08/07/2016	Munich, Germany	LEA – Policy makers	100	International audience
40	Oral presentation at a conference	UNIVERSITY OF WARWICK	4th Cybersec-Cyberdef Conference	14-16/06/2016	Paris, France	Scientific community (higher education, Research) - Policy makers – Industry	300	International audience
41	Organisation of Workshop	GCSEC	Stakeholder validation workshop	19/01/2015	Rome, Italy	Scientific community (higher education, Research) - Industry - Civil society - Policy makers	40	European audience
42	Organisation of Workshop	TECHNISCHE UNIVERSITEIT DELFT	Stakeholder validation workshop	25/01/2016	The Hague, Netherlands	Scientific community (higher education, Research) - Industry - Civil society - Policy makers	40	European audience

43	Organisation of Workshop	UNIVERISTY OF LAUSANNE	Stakeholder validation workshop	30/05/2016	Lausanne, Switzerland	Scientific community (higher education, Research) - Industry - Civil society - Policy makers	25	European audience
44	Organisation of Workshop	UNIVERSITY OF WARWICK	Prevent, Protect, Prepare Workshop	21/03/2017	London, UK	LEA - Industry	40	European audience
45	Organisation of Conference	TRILATERAL RESEARCH LTD	ECRIME final conference	24/03/2017	London, UK	Scientific community (higher education, Research) - Industry - Civil society - Policy makers	45	European audience
46	Press releases	TRILATERAL RESEARCH LTD	ECRIME – Kick-off meeting	01/05/2014	Global audience	Industry	22	Global audience
47	Press releases	TRILATERAL RESEARCH LTD	ECRIME Stakeholder forum formed	01/09/2014	Global audience	Industry	22	Global audience
48	Press releases	TRILATERAL RESEARCH LTD	ECRIME Workshop on Cybercrime Journeys	01/03/2015	Global audience	Industry	22	Global audience
49	Press releases	TRILATERAL RESEARCH LTD	ECRIME Law Enforcement Needs	01/06/2015	Global audience	Industry	22	Global audience

50	Press releases	TRILATERAL RESEARCH LTD	Results of ECRIME citizens survey	01/03/2016	Global audience	Industry	22	Global audience
51	Press releases	TRILATERAL RESEARCH LTD	Report on opportunities for deterring and fighting cybercrime	01/09/2016	Global audience	Industry	20	Global audience
52	Press releases	TRILATERAL RESEARCH LTD	Exploitable outputs from the ECRIME project	01/01/2017	Global audience	Industry	20	Global audience
53	Brochure	INTERPOL	2nd INTERPOL-Europol Cybercrime Conference 2014	01-03/10/2014	Global audience	LEA	230	Global audience
54	Brochure	INTERPOL	11th Heads of National Central Bureaus (NCB) Conference	24-26/03/2015	Global audience	LEA	265	Global audience
55	Brochure	INTERPOL	22nd INTERPOL Asian Regional Conference	15-17/04/2015	Global audience	LEA	160	Global audience
56	Brochure	INTERPOL	2nd Eurasian Working Group Meeting on Cybercrime for Heads of Units	28-30/05/2014	Global audience	LEA	80	Global audience

Section B (Confidential or public: confidential information marked clearly)

LIST OF APPLICATIONS FOR PATENTS, TRADEMARKS, REGISTERED DESIGNS,UTILITY MODELS, ETC.					
Type of IP Rights	Confidential	Foreseen embargo date dd/mm/yyyy	Application reference(s) (e.g. EP123456)	Subject or title of application	Applicant(s) (as on the application)

OVERVIEW TABLE WITH EXPLOITABLE FOREGROUND								
Type of Exploitable Foreground	Description of Exploitable Foreground	Confidential	Foreseen embargo date dd/mm/yyyy	Exploitable product(s) or measure(s)	Sector(s) of application	Timetable for commercial use or any other use	Patents or other IPR exploitation (licences)	Owner and Other Beneficiary(s) involved

ADDITIONAL TEMPLATE B2: OVERVIEW TABLE WITH EXPLOITABLE FOREGROUND	
Description of Exploitable Foreground	Explain of the Exploitable Foreground

4.3 Report on societal implications

B. Ethics

1. Did your project undergo an Ethics Review (and/or Screening)?	Yes
If Yes: have you described the progress of compliance with the relevant Ethics Review/Screening Requirements in the frame of the periodic/final reports?	Yes

2. Please indicate whether your project involved any of the following issues :

RESEARCH ON HUMANS

Did the project involve children?	No
Did the project involve patients?	No
Did the project involve persons not able to consent?	No
Did the project involve adult healthy volunteers?	Yes
Did the project involve Human genetic material?	No
Did the project involve Human biological samples?	No
Did the project involve Human data collection?	Yes

RESEARCH ON HUMAN EMBRYO/FOETUS

Did the project involve Human Embryos?	No
Did the project involve Human Foetal Tissue / Cells?	No
Did the project involve Human Embryonic Stem Cells (hESCs)?	No
Did the project on human Embryonic Stem Cells involve cells in culture?	No
Did the project on human Embryonic Stem Cells involve the derivation of cells from Embryos?	No

PRIVACY

Did the project involve processing of genetic information or personal data (eg. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)?	No
Did the project involve tracking the location or observation of people?	No

RESEARCH ON ANIMALS

Did the project involve research on animals?	No
Were those animals transgenic small laboratory animals?	No
Were those animals transgenic farm animals?	No
Were those animals cloned farm animals?	No
Were those animals non-human primates?	No

RESEARCH INVOLVING DEVELOPING COUNTRIES

Did the project involve the use of local resources (genetic, animal, plant etc)?	No
Was the project of benefit to local community (capacity building, access to healthcare, education etc)?	No

DUAL USE

Research having direct military use	No
Research having potential for terrorist abuse	No

C. Workforce Statistics

3. Workforce statistics for the project: Please indicate in the table below the number of people who worked on the project (on a headcount basis).

Type of Position	Number of Women	Number of Men
Scientific Coordinator	0	1
Work package leaders	4	6
Experienced researchers (i.e. PhD holders)	2	18
PhD student	3	8
Other	13	5

4. How many additional researchers (in companies and universities) were recruited specifically for this project?	10
Of which, indicate the number of men:	6

D. Gender Aspects

5. Did you carry out specific Gender Equality Actions under the project?	No

6. Which of the following actions did you carry out and how effective were they?	
Design and implement an equal opportunity policy	Not Applicable
Set targets to achieve a gender balance in the workforce	Not Applicable
Organise conferences and workshops on gender	Not Applicable
Actions to improve work-life balance	Not Applicable
Other:	

7. Was there a gender dimension associated with the research content - i.e. wherever people were the focus of the research as, for example, consumers, users, patients or in trials, was the issue of gender considered and addressed?	No
If yes, please specify:	

E. Synergies with Science Education

8. Did your project involve working with students and/or school pupils (e.g. open days, participation in science festivals and events, prizes/competitions or joint projects)?	No
If yes, please specify:	

9. Did the project generate any science education material (e.g. kits, websites, explanatory booklets, DVDs)?	No
If yes, please specify:	

F. Interdisciplinarity

10. Which disciplines (see list below) are involved in your project?	
Main discipline:	
Associated discipline:	
Associated discipline:	

G. Engaging with Civil society and policy makers

11a. Did your project engage with societal actors beyond the research community? (if	Yes

'No', go to Question 14)	
11b. If yes, did you engage with citizens (citizens' panels / juries) or organised civil society (NGOs, patients' groups etc.)?	Yes – as part of dissemination
11c. In doing so, did your project involve actors whose role is mainly to organise the dialogue with citizens and organised civil society (e.g. professional mediator; communication company, science museums)?	No
12. Did you engage with government / public bodies or policy makers (including international organisations)	Yes, in communicating /disseminating / using the results of the project
13a. Will the project generate outputs (expertise or scientific advice) which could be used by policy makers?	Yes - as a primary objective (please indicate areas below multiple answers possible)
13b. If Yes, in which fields?	
Agriculture	No
Audiovisual and Media	No
Budget	No
Competition	No
Consumers	Yes
Culture	No
Customs	No
Development Economic and Monetary Affairs	No
Education, Training, Youth	No
Employment and Social Affairs	No
Energy	Yes
Enlargement	No
Enterprise	No
Environment	No
External Relations	No
External Trade	No
Fisheries and Maritime Affairs	No
Food Safety	No
Foreign and Security Policy	Yes
Fraud	Yes
Humanitarian aid	No
Human rightsd	No
Information Society	Yes

Institutional affairs	No
Internal Market	No
Justice, freedom and security	Yes
Public Health	No
Regional Policy	Yes
Research and Innovation	Yes
Space	No
Taxation	No
Transport	Yes
13c. If Yes, at which level?	National and European level

H. Use and dissemination

14. How many Articles were published/accepted for publication in peer-reviewed journals?	4
To how many of these is open access provided?	0
How many of these are published in open access journals?	0
How many of these are published in open repositories?	4
To how many of these is open access not provided?	0

Please check all applicable reasons for not providing open access:	
publisher's licensing agreement would not permit publishing in a repository	NA
no suitable repository available	NA
no suitable open access journal available	NA
no funds available to publish in an open access journal	NA
lack of time and resources	NA
lack of information on open access	NA
If other - please specify	All articles are accessible through open repositories
15. How many new patent applications ('priority filings') have been made? ("Technologically unique": multiple applications for the same invention in different jurisdictions should be counted as just one application of grant).	0

16. Indicate how many of the following Intellectual Property Rights were applied for (give number in each box).

Trademark	0
Registered design	0
Other	0

17. How many spin-off companies were created / are planned as a direct result of the project?	0
Indicate the approximate number of additional jobs in these companies:	0

18. Please indicate whether your project has a potential impact on employment, in comparison with the situation before your project:	Not relevant to the project

19. For your project partnership please estimate the employment effect resulting directly from your participation in Full Time Equivalent (FTE = one person working fulltime for a year) jobs:	not possible to quantify

I. Media and Communication to the general public

20. As part of the project, were any of the beneficiaries professionals in communication or media relations?	No

21. As part of the project, have any beneficiaries received professional media / communication training / advice to improve communication with the general public?	No

22. Which of the following have been used to communicate information about your project to the general public, or have resulted from your project?	
Press Release	Yes
Media briefing	Yes
TV coverage / report	No
Radio coverage / report	No
Brochures /posters / flyers	Yes
DVD /Film /Multimedia	Yes
Coverage in specialist press	Yes
Coverage in general (non-specialist) press	Yes
Coverage in national press	No
Coverage in international press	No
Website for the general public / internet	Yes
Event targeting general public (festival, conference, exhibition, science café)	Yes

23. In which languages are the information products for the general public produced?	
Language of the coordinator	Yes
Other language(s)	No
English	Yes