



# CYBER Security InSURance — A Framework for Liability Based Trust

## Rendicontazione

### Informazioni relative al progetto

#### CyberSure

ID dell'accordo di sovvenzione: 734815

[Sito web del progetto](#)

#### DOI

[10.3030/734815](#)

Progetto chiuso

#### Data della firma CE

15 Novembre 2016

#### Data di avvio

1 Gennaio 2017

#### Data di completamento

31 Dicembre 2021

#### Finanziato da

EXCELLENT SCIENCE - Marie Skłodowska-Curie  
Actions


#### Costo totale

€ 1 647 000,00

#### Contributo UE

€ 1 647 000,00

#### Coordinato da

IDRYMA TECHNOLOGIAS KAI  
EREVNAS  
 Greece

## Periodic Reporting for period 2 - CyberSure (CYBER Security InSURance — A Framework for Liability Based Trust)

Periodo di rendicontazione: 2019-01-01 al 2021-12-31

[Sintesi del contesto e degli obiettivi generali del progetto](#)



Issues addressed in the project:

The CyberSure project aims to develop, monitor, and manage cyber-insurance policies so as to help reduce the risk that cyber systems face and at the same time help educate both insurance companies and system owners of the existing risks and their magnitude and the ways they can reduce them (leading to lowering the insurance cost). The CyberSure goal is to offer a platform of integrated tools, which solves two main problems. Firstly, how to dynamically certify systems continuously that they possess required security properties and/or identify when they do not – similar to adding a GPS tracker on a vehicle to constantly verify that its drivers behave responsibly. Secondly, how to use the information obtained by this continuous, dynamic certification to allow both insurance companies and system owners to improve their understanding of how secure a system really is and thus be able to better calculate the risks associated with security failures.

Importance for Society:

Cyber crime is a fast-growing area of crime in modern society consecutively becoming more aggressive and confrontational. Although cyber insurance's contribution is considered crucial to the holistic addressing of cyber crime, the yet immature respective market faces a number of unique challenges on its way of development. This low maturity of the cyber insurance market leads to poor policy differentiation and customization as well. CyberSure comes to enable cyber insurance market differentiation in the EU, by providing a platform to automate, compare and customize cyber insurance contracts and by facilitating the generation and collection of actuarial data referring to them. Data collection and pooling among insurers and cyber system providers, in particular, is regarded as a prerequisite to generate the knowledge required to differentiate the cyber insurance offer for consumers. By coupling risk assessment to automated certification tools in an automated cyber insurance framework, CyberSure will facilitate the definition of policies and pricing schema making it feasible to be verified and updated dynamically, based on the real time data provided by the risk assessment and hybrid certification mechanisms.

Overall objectives:

The overall aim of CyberSure is to develop an innovative framework supporting the creation and management of cyber insurance policies and offering a sound liability basis for establishing trust in cyber systems and services. To achieve its overall aim, CyberSure undertakes innovation and development activities driven by the following objectives:

Objective 1: To establish a process centric framework for automating the creation and management of cyber insurance policies for cyber systems, based on integrating proven techniques for the certification, audit and risk assessment of security and privacy (S&P) for such systems.

Objective 2: To develop a TRL-5 platform supporting the creation, monitoring and adaptation of cyber insurance policies for cyber systems and the services available through them.

Objective 3: To demonstrate the use of the CyberSure framework in a simulated laboratory environment in the areas of e-health and cloud services and, through them, carry a comprehensive evaluation covering technical, business and legal aspects, and validating the developed technology at TRL-5.

Objective 4: To create conditions for improving cyber insurance practice and the trustworthiness of cyber systems and commercializing the use of the CyberSure platform and framework.

## Lavoro eseguito dall'inizio del progetto fino alla fine del periodo coperto dalla relazione e principali risultati finora ottenuti



During the 2nd Reporting Period (from 01/01/2019 to 31/12/2021), the following work has been achieved:

- M30 WP1: Physical Consortium meeting was held 23 July 2019 in Pisa, Italy.
- M30 WP2: Milestone 4 - Initial Validation of CyberSure Solution, has been achieved.
- M30 WP2: Deliverable D2.4 - Initial Validation of CyberSure Solution, has been successfully completed and delivered, as part of work done in Tasks 2.4 and 2.5.
- M33 WP3: Milestone 5 - Advanced Certification, Risk and Insurance Models, has been achieved.
- M33 WP3: Deliverable D3.1 - Certification, Risk and Cyber Insurance Models, has been successfully completed and delivered, as part of work done in Tasks 3.1 3.2 and 3.3.
- M33 WP4: Milestone 6 - Initial Integrated CyberSure Platform, has been achieved.
- M33 WP4: Deliverable D4.2 - Initial prototype of the CyberSure platform, has been successfully completed and delivered, as part of work done in Tasks 4.2 and 4.3.
- M36 WP1: Physical Consortium meeting was held 5 December 2019 in Nicosia, Cyprus.
- M36 WP5: Milestone 7 - Interim Exploitation and Innovation Plan, and Interim Outreach Workshop, has been achieved.
- M36 WP1: Deliverable D1.4 - Second Project Report, has been successfully completed and delivered, as part of work done in Tasks 1.1 and 1.2.
- M40 WP3: Deliverable D3.2 - Certification, Risk and Cyber Insurance Tools, has been successfully completed and delivered, as part of work done in Tasks 3.4.
- M54 WP1: Virtual Consortium meeting was held 30 June 2021 via teleconferencing.
- M57 WP2: Milestone 8 - Final Validation of CyberSure Solution, has been achieved.
- M57 WP2: Deliverable D2.5 - Final Validation of the CyberSure Solution, has been successfully completed and delivered, as part of work done in Tasks 2.5.
- M60 WP4: Milestone 9 - Final Integrated CyberSure Platform, has been achieved.
- M60 WP4: Deliverable D4.3 - Final prototype of the CyberSure platform, has been successfully completed and delivered, as part of work done in Tasks 4.2 and 4.3.
- M60 WP5: Milestone 10 -Final Exploitation and Innovation Plan, and Final Outreach Workshop, has been achieved.
- M60 WP5: Deliverable D5.3 - Final Exploitation, Innovation, Dissemination and Standardisation Report, has been successfully completed and delivered, as part of work done in Tasks 5.1 5.2 and 5.3.
- Total Secondments for this period: 150,7 person months.

## Progressi oltre lo stato dell'arte e potenziale impatto previsto (incluso l'impatto socioeconomico e le implicazioni sociali più ampie del progetto fino ad ora)



For insuring Cyber Systems, the Risk evaluation process methodology needs to be quantitative and dynamic due to the frequent and fast changes of operational conditions. The CyberSure framework represents a progress beyond the state of the art in regards to Risk Management tools, methodologies and functions. CyberSure aims to develop, monitor, and manage cyber-insurance policies so as to help reduce the risk that cyber systems face and at the same time help educate both insurance companies and system owners of the existing risks and their magnitude and the ways they can reduce them (leading to lowering the insurance cost). The direct potential users of project outcomes includes Cyber Insurers, Cyber System Providers, Certification Authorities as well as the Scientific and Research community, which represent consumers of outcomes for research purposes. It also includes other stakeholders, who may be indirectly affected or have an indirect interest in CyberSure outcomes, including Cyber System user groups, Policy makers and the general public.



CyberSure poster for dissemination at various events

**Ultimo aggiornamento: 9 Settembre 2024**

**Permalink:** <https://cordis.europa.eu/project/id/734815/reporting/it>

European Union, 2025