CyberSure: A Framework for Liability Based Trust

George Christou[1(✉)], Eva Papadogiannaki[1], Michalis Diamantaris[1], Livia Torterolo[2], and Panos Chatziadam[1]

[1] Foundation of Research and Technology Hellas, Heraklion, Greece
{gchri,epapado,diamant,panosc}@ics.forth.gr
[2] Network Integration and Solutions, Genoa, Italy
livia.torterolo@nispro.it

Abstract. CyberSure is a programme of collaborations and exchanges between researchers aimed at developing a framework for creating and managing cyber insurance policy for cyber systems. Creating such policies will enhance the trustworthiness of cyber systems and provide a sound basis for liability in cases of security and privacy breaches in them. The framework is supported by a platform of tools enabling an integrated risk cyber system security risk analysis, certification and cyber insurance, based on the analysis of objective evidence during the operation of such systems. CyberSure develops its cyber insurance platform by building upon and integrating state of the art tools, methods and techniques. The development of the CyberSure platform is driven by certification, risk analysis and cyber insurance scenarios for cyber system pilots providing cloud and e-health services. Through these, CyberSure addresses the conditions required for offering effective cyber insurance for interoperable service chains cutting across application domains and jurisdictions. CyberSure platform aims to tackle the challenges of offering cyber insurance for interoperable service chains cutting across application domains and jurisdictions.

1 Introduction

The establishment of trust across interconnected cyber systems is very important. Widely approved, effective means of managing risks and uncertainty are cyber insurance and security certification. Certification is one way to offer and establish trust relations, since it provides the necessary evidence of the required regular assessment for the provision of a service against security control measures that are explicitly designed to defend against security risks. By definition, insurance enables trust, as it (i) establishes the responsibility of covering reinstating service provision costs following after interruptions or deviations from contractual obligations and/or regulatory standards and (ii) provides compensation for losses, suffered by service consumers due to improper service provision (e.g., loss of personal or commercially sensitive data) [9]. Certification and insurance have been used as instruments for risk mitigation and trust establishment in the provision of a wide spectrum of services and industries, such as construction services,

© Springer Nature Switzerland AG 2020
A. P. Fournaris et al. (Eds.): ESORICS 2019 Workshops, LNCS 11981, pp. 19–34, 2020.
https://doi.org/10.1007/978-3-030-42051-2_2

health services, hospitality services, and services in the banking sector. Moreover, for several types of such systems and services, providing certification and insurance is being mandated through legislation and regulations, as for instance in the case of health services, energy systems, vehicle maintenance systems and services, and shipping and logistics services. From the insurance perspective, offering cyber security certifications is a valid way to demonstrate that certain security controls have been implemented using the necessary standards. More specifically, in domains like online shopping, tourism services and pharmacies, we can observe a significant effect derived by the establishment of certification and cyber insurance. There have been several studies that indicate the ever increasing importance of cyber insurance, globally, as well as the challenges that occur. For instance, recent surveys present trends in the European Union cyber insurance market, including (i) fast expansion, (ii) significant investment and (iii) dramatic increase in cyber insurance costs and premiums.

Revenue opportunities resulted by cyber insurance can be achieved through meaningful cost savings. One solution is to take advantage of techniques that are able to produce accurate risk assessments, behaviour-based insurance contracts and dynamic pricing. In addition, having the ability to handle diverse consumer technology and fluctuations in legislations is necessary. Apparently, these trends require dynamic and automated establishment, management and adaptation of cyber insurance policies, including dynamic risk assessment and dynamic pricing. In addition, costs required to acquire customers can be reduced using analytics and increased insurance customisation to the characteristics of the subject of insurance. Still, all these requirements are not effectively addressed. More specifically, certification is yet based on labourintensive inspection and periodic offline testing of cyber systems and it does not strictly guarantee the preservation of every certified property between the certification audits. Furthermore, since the risk estimation and creation of cyber insurance policies happen during asynchronous periodic time periods, they are not able to effectively account for intermediate changes between these systems. Currently, risk estimation and creation of cyber insurance contracts are not able to consider fine-grained operational evidence obtained through monitoring and testing of cyber systems. Consequently, risk estimations are not accurate and, thus, insurance policies might not be effective for any of the entities associated.

CyberSure is an European Unions Horizon 2020 research and innovation programme (H2020-MSCA-RISE-2016). The project consortium comprises the following institutions and organizations: Foundation for Research and Technology - Hellas (FORTH), City University (CITY), Italian National Research Council (CNR), Cablenet, Hellas Direct, and Network Integrated Solutions S.r.l. (NIS). In paper, we present CyberSure, a framework that supports the creation and management of cyber insurance policies in order to establish trust in cyber systems and services. This framework is supported by a platform of integrated tools that enable: (i) the dynamic certification of security and privacy properties of cyber systems and services that need to be insured, (ii) the dynamic estimation of security and privacy risks for such systems and services, and finally, (iii) the

development, monitoring and management of cyber insurance policies for these systems and services.

The main objectives of CyberSure are:

- 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
- To develop a platform supporting the creation, monitoring and adaptation of cyber insurance policies for cyber systems and the services available through them
- To demonstrate the use of the CyberSure framework in real world trials in the areas of e-health and cloud services and, through them, carry a comprehensive evaluation covering technical, business and legal aspects, and demonstrating technology readiness
- To create conditions for improving cyber insurance practice and the trustworthiness of cyber systems and commercialising the use of the CyberSure platform and framework.

2 Related Work

In this section we present the various processes and components associated with Cyber Insurance. We discuss the current state of the art regarding each process and what are the main innovations of CyberSure framework.

2.1 Security Certification

Security certification is a way to evaluate and certify than a cyber infrastructure is in line with security standards [14]. The certification process results in a certificate, stating that an ICT system is compliant with a certification scheme, which defines the security properties and standards that should be complied with. The evaluation of the infrastructure can be either self assessed, i.e. the process is carried out by the owner of the infrastructure, or be conducted by a third-party organisation, i.e. a certification lab.

A notable certification scheme which spans certification process from the early stages of development up to the evaluation of the final infrastructure is the Common Criteria for Information Technology Security Evaluation [13]. Common Criteria evaluation results in a rating against an Evaluation Assurance Level (EAL). EALs are characterised by:

- The types of evidence that have been taken into account for evaluation (e.g., inspection, testing, formal verification).
- The agent who carried out the evaluation.
- The documentation/evidence that has to be produced and assessed for a successful evaluation.

There are numerous ISOs for information security standards. For example ISO/IEC 27001:2013 [6] dictates that the infrastructures information security risks will be examined systematically taking into account possible vulnerabilities, threats as well as possible impact of incidents. Moreover, an adequate set of information security controls will be designed and implemented in order to avoid and treat unacceptable risks. Finally, due to emerging threats, a management process must ensure that the information security controls are frequently updated in order to meet the infrastructures information security goals.

Despite the vast number of different approaches and certification that are available for the vast majority of IT ecosystems, the process is not automated and the evaluation relies on manual inspection with limited support from inspection tools. The EU project CUMULUS was designed to address these issues when it comes to certification. It is mainly used to automatically apply different types of certification schemes. Possible schemes can be based on data acquired by testing and monitoring.

CyberSure will explore possible ways in order to combine certification and risk management with cyber insurance. For this purpose, CUMULUS certification models will be developed and by automatically applying them to cyber infrastructures risk estimates, insurance policies and premiums will be dynamically adjusted. Thus, through the continuous monitoring and testing it will be possible to access the certification compliance of an infrastructure dynamically. Continuous monitoring is accomplished by deploying event captors at the client infrastructure which are responsible for transmitting certification evidence to CUMULUS monitors in a confidential manner (i.e. secure communication).

2.2 Risk Assessment and Management

Due to the continuously increasing criticality and complexity of cyber infrastructures, several methods and tools have been proposed with regards to risk assessment. The main challenge that is tackled by risk assessment is to identify and narrow down the possible cyber-attack events that could severely impact the operation of a cyber infrastructure. Part of effective risk assessment is the discovery of possible attack vectors. There are risk assessment strategies, which rely on high-level descriptions of the process that should be followed to identify risks and are not algorithmic. On the other hand, there exist more technical strategies, which provide tools in order to automate parts of the process.

A notable example of generic risk assessment methods is OCTAVE [7]. OCTAVE is mostly driven by operational risks and critical assets of an organization. At first, possible impact areas are identified (e.g. safety, health, etc.). The next step is to identify the critical information assets of the organization. The assets are categorized depending on the value and how depended is the operation of the infrastructure to that asset. At this step, the security requirements of each asset are also identified. Each asset that processes data is considered an information asset container. Beyond the outcome of a possible attack, an estimation of the consequences in case the threat scenario happens is calculated. The potential threats are then represented in threat trees. In order to assist with the traversal of the threat trees, OCTAVE provides worksheets and questionnaires.

Impact areas are then ordered in terms of severity depending on how many of the realized threats can affect them. Finally, a mitigation approach is decided for each risk. A risk can be mitigated, avoided, deferred or even accepted.

MAGERIT [2] is another method which follows a similar approach. Initially, informations regarding the assets of the infrastructure, the inter-connections between them and their value are collected. For each one of the assets et of possible threats is determined and already available safeguards are analysed in terms of effectiveness mitigating the risks. Next, the damage to an asset and the expected rate of occurrence of each threat is estimated. At the final step, for each risk, a treatment is decided. A risk can either be accepted and a monitoring scheme will be deployed in order to capture the occurrence of such risk, or treated. Treatment options include avoiding the risk by eliminating the source of the risk from the infrastructure, mitigating the risk by deploying mechanisms which can effectively reduce the impact and the likelihood of the threat, sharing the risk by outsourcing system components or using cyber-insurance, and finally fund the risk i.e. reserving funds in order to cover the impacts of the risk.

Other frameworks, such as MEHARI [1], combine a knowledge base created using MEHARI and adhere to the organization the risk management proposed by ISO 27002:27005. By creating the knowledge base of the infrastructure, the risk assessment can be tailored to the specific use case. The representation of the knowledge base offers the ability to develop a set of tools that will enhance the risk assessment. Moreover, risks can be analyzed in terms of events that can lead to each situation. When the risk assessment process is complete, decisions can be made with regards to what security measures should be implemented in order to assure that possible risk impacts are within acceptable margins. Finally, provided tools can be also used in order to assist security management over time by monitoring accepted risks.

More quantitative and tool based approaches like CORAS [10], provide customized language for modeling the risks and threats. CORAS is a framework for model-based security risk analysis consisting of a language, a method, and a tool. The language provides a graphical representation of main concepts and the relations between them. The method realizes an asset-driven defensive risk analysis and is supported by the tool implementing the language. The main concepts of risk assessment (such as threat agents, threats, vulnerabilities, impact, assets, etc.) are represented as nodes of specific types and are connected with the relations between them. Quantitative or qualitative values may be assigned to the nodes and relations for risk evaluation. The Unified Modeling Language (UML) is typically used to model the target of the analysis. The CORAS method provides a computerized tool designed to support documenting, maintaining and reporting analysis results through risk modeling.

In CyberSure risk assessment is part of the validation framework. Part of of the process ensures that the components of the system cooperate without side effects and that the business goals are achieved. The main innovation of the CyberSure framework is the semiautomatic way of collecting the information about the security risk level of the infrastructure. As described in this section, risk assessment relies mostly on questionnaires and highly generic methods, while

there is only a small number of solutions that offer automation through tools (e.g. modeling languages). This is particularly cumbersome for insurance companies since, the data collected from such methods are coarse-grained The CyberSure framework integrates a certification checking module (CUMULUS [19]), which is able to validate part of this information. Finally, our proposed risk assessment process helps to quickly process the data and estimate the possible losses for an insurance company.

2.3 Insurance

Cyber Insurance is a quite new product offered by insurance companies, thus it still faces critical challenges [17]. The main challenge is that there are i not enough data regarding the assesment of cyber security incidents in order to produce accurate statistic conclusions. Since, data related to cyber security insidents are usually very sensitive and thus, companies avoid to disclose and share them with third parties. However this issue is mitigated in Europe through the Directive on security of networks and information systems [16].

Another major challenge originates from the fundamental properties of technology. The rapid evolution of both the systems and attacks and the complex interdependencies between cyber infrastructures assets impede the accurate identification and impact assessment of cyber risks [4]. Moreover, the cyber insurance coverage is inherently hard to define and the exceptions and correctness of the policy is more legal oriented than technological. Despite the challenges and the immaturity of cyber insurance services has a positive influence on cyber security [5].

In CyberSure, the automated security and risk assessment and dynamic certification will be used in order to develop a novel tool which will be able to tackle the challenges of cyber insurance. Insurance policies will be able to apply certification processes and depending on the results, specific risks will be highlighted in order to be covered. The automated processes will reduce the information asymmetries and will simplify the identification of interdependencies. Moreover, the quantitative risk assessment will process the evidence data and estimate the possible losses for the insurance company. Finally, the insurance component will select best pricing strategy.

3 Design

One of the main key challenges of CyberSure is to integrate proven state-of-the-art techniques in certification, risk assessment and insurance management into a unified framework for the management (i.e., creation, pricing, monitoring and adaptation) of cyber insurance policies for cyber systems. As can be seen in the architecture overview in Fig. 1, CyberSure develops a platform incorporating three basic components; (i) a certification infrastructure (supporting phase `Certification`), (ii) a risk management tool (supporting phases `Baseline risk analysis` and `Comprehensive risk assessment`) and (iii) the insurance management tools (supporting `Cyber insurance policy management` phase).

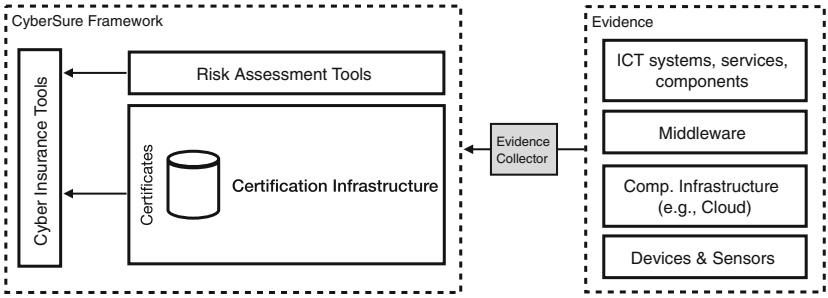

Fig. 1. The CyberSure framework.

This integration will be based on a generic process for cyber insurance management, which will orchestrate activities focusing on cyber systems risk modeling, certification, and cyber insurance policy management. This process supports integration by defining the expected data flows and interfaces between the activities of risk modeling, certification and cyber insurance management. Moreover, it supports both qualitative and quantitative types of analysis of cyber systems assurance at different levels and can be tailorable to the needs of individual service providers and insurers. As can be seen in Fig. 2, CyberSure's generic process for cyber insurance management involves the following four phases:

- `Baseline risk analysis.` Risk assessment methodologies and tools support the early analysis and specification of risk models, i.e., high level models of threat agents and attacks that may pose different types of risks to cyber system assets as well as the possible countermeasures that may be used to mitigate these risks.
- `Certification.` Based on the risk models developed in the previous phase, the CyberSure framework will generate executable cyber system certification models and use them to carry out assessments of the soundness and the effectiveness of the security controls that are used in such systems for mitigating risks. These assessments may be fully or semi-automated and will be based on static or dynamic testing, such as penetration testing, and/or continuous monitoring of the mechanisms of cyber systems, depending on the underpinning certification models. Depending on the outcomes of such assessments, certification may generate digital certificates providing basic risk level guarantees required for cyber insurance. This phase also generates the detailed operational evidence that underpins certificates as an additional means for assessing risks in cases where certificates won't be sufficient for risk assessment in the context of managing cyber insurance policies.
- `Comprehensive risk assessment.` The certificates and the operational evidence generated by `Certification` provide inputs to a subsequent comprehensive assessment of risk that may be required for formulating and pricing cyber insurance policies. The calculation of cyber system exposure to risk is probabilistic and is based on the analysis of the historic detailed evidence provided by certification. Calculating risk exposure is dynamic and makes

use of the outcome of continuous certification. Moreover, this phase will also involve the evaluation of the impact of risk on cyber system providers, such as the impact on business reputation, the theft of intellectual property, as well as the cost of eliminating it.

– `Cyber insurance policy management.` This phase covers the activities of managing cyber insurance contracts, such as policy creation, pricing, updating and claim handling, and will use inputs from previous phases. For example, Cyber system assets that have been identified as vulnerable to particular threats in phase `Baseline risk analysis`, will be the candidate subjects of insurance and may be used for customized policy creation and updates. The certificates and continuous operational evidence generated in phase `Certification` may be used as prerequisites for continuous policy validity checks. Furthermore, the cyber system assets risk exposure and impact estimates generated in phase `Comprehensive risk assessment`, may be used for policy pricing. The `Cyber insurance policy management` phase will also provide feedback to earlier phases. This feedback will arise from an analysis of claims referring to compromised assets across different policies, which may indicate the need to revise threat and certification models (used in phase `Baseline risk analysis` and `Certification`, respectively) and/or the risk exposure and the impact estimation methods used in `Comprehensive risk assessment`.

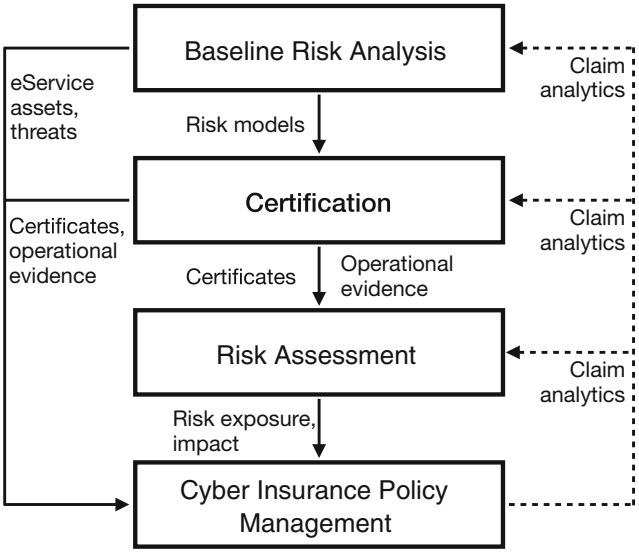

Fig. 2. CyberSure's generic process for cyber insurance management.

3.1 CyberSure's Internal Mechanisms and Tools

In this section we describe the tools incorporated and used for each one of the three basic components as well as relationship between them, as can be seen in Fig. 1.

Certification Infrastructure. The certification infrastructure integrated in the CyberSure platform has been developed by the EU F7 R&D project CUMULUS (Certification infrastrUcture for MUlti-Layer cloUd Services) [3,12,19]. This infrastructure can be used to define and execute automatically certification models. These certification models specify the security and privacy properties required of cloud services; how to acquire and analyse evidence in order to assess whether the provision of services satisfies these properties, and how to generate certificates that confirm the compliance of services with the required properties. Moreover, the CUMULUS infrastructure supports the collection and analysis of different types of evidence, including both static and dynamic test data. The data collection includes continuous monitoring data for cloud service provision, as well as data gathered from trusted platform modules that can guarantee the integrity of the software components, which are used to realize the services and the countermeasures against threats. The test and monitoring data that are required by a certification model in order to assess security properties are acquired by evidence collectors built into the software components that realize the services and/or the computational platforms where these services are deployed on (e.g., the cloud). To address the objectives of CyberSure, the CUMULUS certification models and infrastructure will be extended to support the specification of certification models that are based on unified concepts with the risk models used in phases `Certification` and `Cyber insurance policy management` of the general CyberSure process regarding the service assets, threats, and security countermeasures.

Risk Assessment Tools. The risk assessment tool RiS (Risk Integrated Service) integrated in the CyberSure platform has been developed by CNR (The Italian National Research Council) in order to support Information Security and IT Risk Management consulting services. CNR provides a a web-based solution that implements a risk process, based on ISO 31000 standard, that is able to assess, evaluate and manage IT risks of assets in scope. The main parameters analyzed are the asset severity, the threats and their probability of occurrence and the vulnerabilities. The `Risk assessment tools` is already able to provide a high-level risk scenario starting from a template of a predefined threats and vulnerabilities. We will also extend the functionalities provided in order to also support the `Comprehensive risk assessment` phase which requires the development of a new model able to calculate the cyber system exposure to risk on a probabilistic base and making use of historic/operational evidences provided by certification. In order to be consistent with the evolving threat and vulnerability landscape and to dynamically report on the increased levels of risk, this tool will integrate and correlate the outcome of the continuous certification process. Finally, it will be also extended to provide a cost-benefit analysis by exploiting the NeSSoS (Network of Excellence on Engineering Secure Future Internet Software Services and Systems) risk, cost management and assurance framework. NeSSoS also benefits from cooperation with the CUMULUS tool on acquiring the real evidence of the security configuration of the system and helping the

insured customers to fill in the required input data, as well as verifying the correctness of the data provided.

Insurance Management Tools. The insurance management tools that will be integrated in the CyberSure platform derive from the main tools already adopted by HELLAS-DIRECT in managing insurance products in non-life insurance. These tools have the purpose of defining a price for the policy in order to fulfill the needs of the insured together with the target of the company, taking into account the updated risk profile of the insured. To achieve this goal, historical data conveniently classified will be given as the input of the models will allow the company to reach their targets, while also applying discounts or penalizations. The existing tools will be extended and modified in order to receive and integrate, as inputs, the outputs of the `Comprehensive risk assessment` and `Certification infrastructure`. The complete process and the tools used will be tailored according to the needs of the individual service providers and the insurers, since the goal of CyberSure is to support both complex cyber insurance scenarios that require automated certification as part of cyber insurance policy issuing and management but also simpler scenarios where certification might be performed in a non automated manner or not required at all.

3.2 Monitoring and Pricing Components

The CUMULUS framework facilitates the collection and analysis of different types of evidence and continuous monitoring of data, as well as data gathered from trusted platform modules that can guarantee the integrity of the software components. The monitoring data that are processed by a certification model, in order to evaluate the system properties, are acquired by evidence collectors deployed on the software components of the pilot systems, the health-care organization and the cloud provider, respectively.

The pricing component takes multiple inputs and estimates the pricing of each cyber insurance policy. The main input is the CyberSure comprehensive risk score, calculated using the previous components of the CyberSure platform, RiS and NeSSoS and the monitoring component by CUMULUS. The revenue of the company purchasing the policy affects the premiums in a positive way, since the higher the value of generated revenue, the higher the economic damage a possible cyber incident can have on the bottom line of the company. The critical dependency of business processes on IT, i.e. how a potential IT interruption would lead to a business interruption as well, is another factor affecting pricing. Past claims have been shown to be positively associated with future claims, and hence they are taken into account in pricing for cyber insurance. The specific industry and non-profit status of the company also affect the perceived risk of cyber incidents requiring pricing adjustments. Moreover, the type of data collected about customers, and whether this includes any sensitive personal data, has a quantifiable effect on pricing. Limits of insurance coverage, i.e. the maximum amount the insurance company will cover, and deductible amounts, i.e. the amount the insured party needs to cover before the insurance company starts paying their share, are two extra components of pricing [11,15,18].

4 Validation

In this section we discuss the validation procedure for the CyberSure framework [8]. CyberSure's validation process consists of a combination of three steps: (i) the technical, (ii) the business and (iii) the legal validation. Regarding the technical validation step, we will focus on assessing the integration of the standalone tools (i.e. CUMULUS, NESSOS, RIS and the pricing module), showing that the CyberSure platform as a whole works effectively from a technical point of view. Regarding the business validation step, the procedure aims to evaluate the business idea of the project, assessing the profitability and sustainability of the business model in respect to market and customer attractiveness. Finally, considering the legal validation step, the validation procedure aims to verify the platforms compliance with every European and national regulations, including GDPR. So far, CyberSure is under an initial validation state.

4.1 Criteria

In this section we define a set of different criteria that we aim to verify in order to ensure the quality of projects' outcomes. We divide these criteria into three categories: (i) technical, (ii) business and (iii) legal criteria. In the following paragraphs we discuss the aforementioned criteria.

Technical Criteria. From a technical point of view, CyberSure has to be validated in terms of methodology, software components, infrastructure, integration and communication. Since the CyberSure framework consists of a number of standalone tools, the validation of the platform has to be considered as an integration of the validation process of the tools. As already discussed, the main modules involved are: (i) CUMULUS, (ii) RIS, (iii) NESSOS and (iv) the pricing module. CUMULUS is a tool that is used to monitor security controls of IT infrastructures. The RIS service is a web application which relies on a database, hosted on the same server. The NESSOS tool is a web-based application that aims to evaluate risks of an organization. Finally, the pricing module is developed to estimate the price for various cyber insurance products, based on the input provided by other components of the CyberSure platform, the prices on similar products in the market and any additional factors that may be taken into account. Consequently, we need to verify that the evaluated pilot systems can interact with the proposed CyberSure platform and enable the real-time monitoring of the underlying assets.

As a result, for each one of the tools, the technical key factors to be evaluated include the following:

- *CUMULUS*: Ability to install, configure, and operate the event captors to the pilot system.
- *CUMULUS*: The minimum disruption of the functionality of the main pilot hardware and software by the CyberSure monitor.

- *CUMULUS*: Ability to create a secure environment that will include authorization and authentication of different event captors before transmitting events to CUMULUS. This will prevent CUMULUS from receiving and analyzing events which were not transmitted from one of the Pilots.
- *RIS*: The RIS service relies on an Oracle Database and Oracle Application Express technology. The factors that must be considered in the validation of the process of risk assessment are: authentication and authorization mechanisms, reliability of input parameters, risk outcomes coherence and security.
- *RIS*: RIS's servers virtual infrastructure must be analyzed and evaluated.
- *RIS*: The RIS service must be provided in SaaS and the availability of the service must be analyzed and validated.
- *NESSOS*: Factors that need to be considered for the validation of the NESSOS tool are: Authentication and authorization, reliability of input parameters, risk outcomes coherence and security.
- *NESSOS*: For a reliable and secure execution of the NESSOS tool, it must be ensured that the infrastructure is reliable and secure, as well.
- *NESSOS*: Since the NESSOS tool must be integrated with other modules of the platform availability and correct integration with the other tools of the CyberSure platform, need to be validated, as well.
- *Pricing Module*: Regarding the software validation, some of the factors that must be considered are: authentication and authorization mechanisms, reliability of input parameters, reliability of products and prices of similar cyber insurance products, policy outcomes coherence and security.
- *Pricing Module*: Pricing Module's servers virtual infrastructure must be analyzed and evaluated.
- *Pricing Module*: The Pricing module must be integrated with other modules to receive inputs from the baseline and the comprehensive risk assessment, receive competitors' product and pricing intelligence from the market and must provide proper and adequate policies to the insurance company.

Business Criteria. The main objective of business criteria for validation is to assess the appeal of cyber insurance products and associated services in the market, as well as to define the value proposition of the platform that would allow us to capture enough market share to make the project financially viable. In addition, a very important goal is to be able to forecast the future market performance of the platform from the insurance point of view, and how the platform can be used to estimate the risk for cyber threats and, hence, adjust the pricing of insurance policies.

The key business factors for a successful cyber insurance business include the profitability of the underwriting models, the customer attractiveness of the cyber insurance products and the cuber risk score. The profitability of the underwriting models is defined as the total amount of insurance premiums collected from insured, subtracting the amounts claimed by the insured due to events that have affected the insured business as prescribed in the insurance agreement. The customer attractiveness of the cyber insurance products is based on a variety of

factors, the main of which are the price, relatively to the competition and the insured value (sum assured), and the coverage of the insurance (i.e. under which events/circumstances would the cyber insurance reimburse the insured for their losses). Additional factors that contribute to the customer attractiveness is the ease of policy acquisition, the ease of the claims procedure and the availability and type of customer service (phone, chat, email, on-site, technical, 24-h). The CyberSure platform aims to aid the customer attractiveness process by estimating more accurately than the competition, and in a more robust and automated way, the cyber risks and expected economic value of the insured events, allowing the insurer to lower the insurance premiums. The cyber risk score, the main output of the CyberSure platform, will be calculated using semi-automated tools, developed by the CyberSure collaboration, and can be monitored by both the insurer and the insured continuously. Risks are taken into account depending on their economic value and their probability of occurrence, and are frequently re-evaluated to include new cyber risks or attacks that become possible as technology progresses. The insurance needs consist of the method to estimate the cyber risk of the customers, both in terms of the magnitude of the expected economic effect and of the expected frequency of each event. Utilizing the output from the CyberSure platform, and taking into account the cyber insurance market prices and the desire and prospect for growth of the company portfolio, the insurance company will price each prospective customer accordingly.

The evaluation of the key business criteria will be determined by two main factors: the market penetration and the profitability of the business. The market share of the cyber insurance products should be respectable, in order to have the cyber insurance line deemed successful. In addition, the brand awareness of the cyber insurance line should be such that potential that customers would consider this opportunity, even if they will not purchase in the end. The profitability of the business will be shown in the medium term, after cyber insurance claims have been filed and the cyber insurance line is profitable, after accounting for the claims, and the operating expenses, as well.

Legal Criteria. The main objective of legal criteria for validation is to verify that the platform CyberSure is compliant with all European and national laws and regulations, including GDPR. The development of the legal criteria includes the following steps: (i) the analysis of the legal landscape, in relevance to CyberSure, (ii) the awareness of the data and its nature and sensitivity, (iii) the application of certain principles on data quality, purpose specification, use limitation, security safeguards, practices and policies openness, individual participation and accountability. Finally, CyberSure takes its responsibilities under the GDPR and the requirement to treat personal information in an appropriate and lawful manner very seriously and as such, complies with the data protection principles.

4.2 Applications

To validate CyberSure, two different scenarios of cyber insurance will be used. The first validation scenario will be based in the e-health area, while the second

scenario will be based in the cloud systems and services. These two scenarios involve different implementation platforms and critical security and privacy requirements to be insured. Successful deployment of CyberSure in these two distinct cyber ecosystems will validate the effectiveness of our framework. Moreover, during the deployment phase, CyberSure will be refined through the lessons learned during this process.

In the first scenario, we will use an IT software that is used in the healthcare domain. More specifically, this software focuses on integrated health-care solutions in the wider context of predictive, individualized, preventive and participatory medicine. The most major security, privacy and dependability requirements are: (i) the preservation of privacy, confidentiality and integrity of medical records in-transit and at-storage, (ii) the preservation of privacy, confidentiality and integrity of prescription and financial data in-transit and at-storage, and (iii) the preservation of a high degree of the e-health platform availability. In the second scenario, we will use the Datacenter Virtual Infrastructure (DVI) of Cablenet, an ISP that participates in the CyberSure project as member of the consortium. DVI is physically protected a number of protection measures focusing on physical access, power-related risks, air conditioning and fire suppression. The main security and privacy requirement for the cloud scenario is the fact that all data must be encrypted to remain confidential both in transit and at-storage. Furthermore, data integrity and privacy are highly required, while application integrity and availability need to be ensured. Thus, there must be mechanisms monitoring and reporting any abnormalities and breaches in the cloud services. Notifications of security breaches to system administrators and potentially the users should also be supported.

5 Conclusions

In this paper, we present the major objectives of the CyberSure project. CyberSure is a framework for liability based trust, supported by a platform of tools enabling an integrated risk cyber system security risk analysis, certification and cyber insurance, based on the analysis of objective evidence during the operation of such systems. The development of the CyberSure platform is driven by certification, risk analysis and cyber insurance scenarios for cyber system pilots providing cloud and e-health services. So far, the validation progress of the CyberSure project is in an initial state, as discussed in the corresponding section. As future work, we plan to publish the results and details of the validation progress, after its completion.

Acknowledgements. This work was supported by the European Commission through the project CONCORDIA Horizon 2020 Research and Innovation program under Grant Agreement No. 830927 and CYBERSURE Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Grant Agreement No. 734815.

References

1. Mehari 2010: risk analysis and treatment guide. club de la securite de l'information francias, August 2010. [cm03] C. Copeland J. Moteff, Science John Fischer Resources, and Industry Division
2. Amutio, M., Candau, J., Mañas, J.: Magerit-version 3, methodology for information systems risk analysis and management, book I-the method. Ministerio de Administraciones Públicas (2014)
3. Anisetti, M., Ardagna, C.A., Damiani, E.: A certification-based trust model for autonomic cloud computing systems. In: 2014 International Conference on Cloud and Autonomic Computing, pp. 212–219 (September 2014). https://doi.org/10.1109/ICCAC.2014.8
4. Böhme, R., Schwartz, G., et al.: Modeling cyber-insurance: towards a unifying framework. In: WEIS (2010)
5. Bolot, J., Lelarge, M.: Cyber insurance as an incentivefor internet security. In: Johnson, M.E. (ed.) Managing Information Risk and the Economics of Security, pp. 269–290. Springer, Boston (2009). https://doi.org/10.1007/978-0-387-09762-6_13
6. Calder, A., Watkins, S.: IT Governance: An International Guide to Data Security and ISO27001/ISO27002. Kogan Page Publishers, London (2012)
7. Caralli, R.A., Stevens, J.F., Young, L.R., Wilson, W.R.: Introducing OCTAVE Allegro: improving the information security risk assessment process. Technical report, Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst (2007)
8. CyberSure: Deliverable D2.2: CyberSurevalidation framework. http://www.cybersure.eu/m/filer_public/15/e4/15e47988-2b90-4828-ae63-4a4c4c9ccef3/cybersure_-_d22_final.pdf. Accessed 05 July 2019
9. Enisa: Incentives and barriers of the cyber insurance market in Europe. https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe. Accessed 05 June 2019
10. Fredriksen, R., Kristiansen, M., Gran, B.A., Stølen, K., Opperud, T.A., Dimitrakos, T.: The CORAS framework for a model-based risk management process. In: Anderson, S., Felici, M., Bologna, S. (eds.) SAFECOMP 2002. LNCS, vol. 2434, pp. 94–105. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-45732-1_11
11. Innerhofer-Oberperfler, F., Breu, R.: Potential rating indicators for cyberinsurance: an exploratory qualitative study. In: Moore, T., Pym, D., Ioannidis, C. (eds.) Economics of Information Security and Privacy, pp. 249–278. Springer, Boston (2010). https://doi.org/10.1007/978-1-4419-6967-5_13
12. Katopodis, S., Spanoudakis, G., Mahbub, K.: Towards hybrid cloud service certification models. In: 2014 IEEE International Conference on Services Computing, pp. 394–399, June 2014. https://doi.org/10.1109/SCC.2014.59
13. Kruger, R., Eloff, J.H.P.: A *Common Criteria* framework for the evaluation of information technology systems security. In: Yngström, L., Carlsen, J. (eds.) Information Security in Research and Business. ITIFIP, pp. 197–209. Springer, Boston (1997). https://doi.org/10.1007/978-0-387-35259-6_16
14. Lagazio, M., Barnard-Wills, D., Rodrigues, R., Wright, D.: Certification schemes for cloud computing. EU Commission report (2014)
15. Marotta, A., Martinelli, F., Nanni, S., Orlando, A., Yautsiukhin, A.: Cyber-insurance survey. Comput. Sci. Rev. **24**, 35–61 (2017). https://doi.org/10.1016/j.cosrev.2017.01.001. http://www.sciencedirect.com/science/article/pii/S1574013716301137

16. Nikolopoulou, A.: The directive on security of networks and information systems (NIS Directive) from a practical view (2019)
17. Podolak, G.D.: Insurance for cyber risks: a comprehensive analysis of the evolving exposure, today's litigation, and tomorrow's challenges. Quinnipiac L. Rev. **33**, 369 (2014)
18. Romanosky, S., Ablon, L., Kuehn, A., Jones, T.: Content analysis of cyber insurance policies: how do carriers price cyber risk? J. Cybersecur. **5**(1) (2019). https://doi.org/10.1093/cybsec/tyz002
19. Spanoudakis, G., Damiani, E., Mana, A.: Certifying services in cloud: the case for a hybrid, incremental and multi-layer approach. In: 2012 IEEE 14th International Symposium on High-Assurance Systems Engineering, pp. 175–176. IEEE (2012)