@H2020Secondo

@H2020Secondo

SECONDO Project

Secondo Project

For more information, please visit our site: secondo-h2020.eu

SCAN ME

CONSORTIUM

1 UNIVERSITY OF PIRAEUS

1 UBITECH ubiquitous solutions

1 FOGUS INNOVATIONS & SERVICES

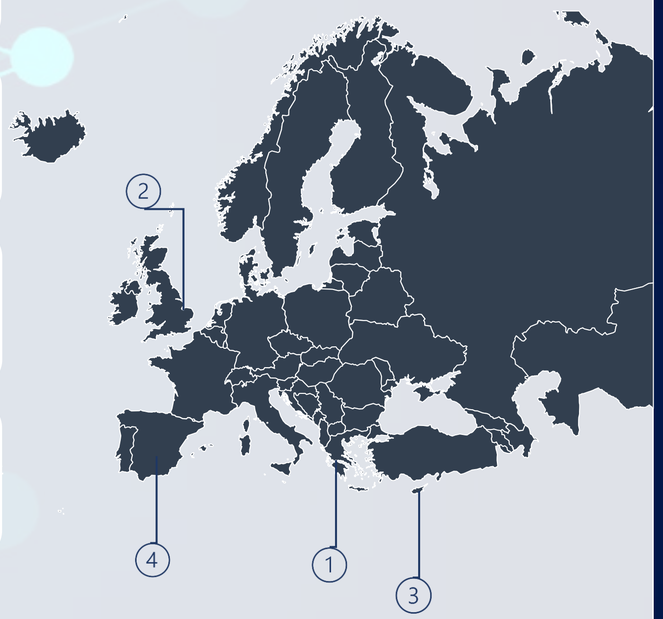
1 CROMAR INSURANCE BROKERS LTD

2 UNIVERSITY OF SURREY

2 UNIVERSITY of GREENWICH

3 Cyprus University of Technology

4 LS TECH Insightful Analytics



PROJECT COORDINATION

Prof. Christos Xenakis: School of Information and Communication Technologies Department of Digital Systems University of Piraeus Karaoli and Dimitriou 80,PC 18534, Piraeus, Greece

Tel: +30 210 4142776
email: xenakis@unipi.gr

This project has received funding from the European Union's H2020-MSCA-RISE-2018 program under grant agreement No 823997.

SECONDO

"A Security ECONomics service platform for smart security investments and cyber insurance pricing in the beyonD 2020 netwOrking era"

PROJECT DETAILS

Project number: 823997
Project Website: secondo-h2020.eu
Project start: 1st January 2019
Duration: 48 Months
Total cost: EUR 1 600 800
EC Contribution: EUR 1 600 800

Cyber Insurance Challenges

Cyber insurance is a hybrid ecosystem combining features from classic insurance and information technology and inherits challenges from both sectors. Below, the identified challenges that the cyber insurance ecosystem faces are presented.

- CH1—Lack of data
- CH2—Lack of automated tasks
- CH3—Fraudulent claims
- CH4—Identity theft
- CH5—Loss of sensitive data
- CH6—Know your customer
- CH7—Information asymmetry
- CH8—Interdependent and Correlated Risks
- CH9—Premium Calculation

The essential stakeholders in cyber insurance are further elaborated below In a nutshell, a Policyholder (PH) is a holder of cyber insurance and a customer to an Insurance Company (IC). The latter is a stakeholder responsible for selling cyber insurance policies to potential PHs, investigating a cybersecurity incident, and auditing whether the PHs comply with the cyber insurance policies and have implemented the indicated cybersecurity countermeasures. Additionally, Cyber Insurance Brokers (CIBs) perform market research and bring the most suitable contracts to their PHs. Below, the cyber insurance processes are presented:

- CIP1—Market research
- CIP2—Client registration and validation
- CIP3—Underwriting
- CIP4—Pricing premium
- CIP6—Claims submission
- CIP7—Claims validation and auditing
- CIP5—Periodic risk assessment

Why will SECONDO integrate Blockchain

Blockchain is a decentralized and distributed ledger technology that revolutionizes record-keeping by offering secure, transparent, and tamper-resistant transactions across a network of computers. Its key features include **decentralization**, eliminating the need for a central authority, and **immutability**, ensuring once data is added to a block, it becomes nearly impossible to alter. **Transparency** is inherent, with all participants having access to the entire ledger, though individual identities remain pseudonymous. The blockchain's **security** is bolstered by cryptographic techniques and consensus mechanisms, safeguarding against fraud and hacking. The distributed ledger is **replicated** across all network nodes, enhancing data integrity and resilience against single points of failure.

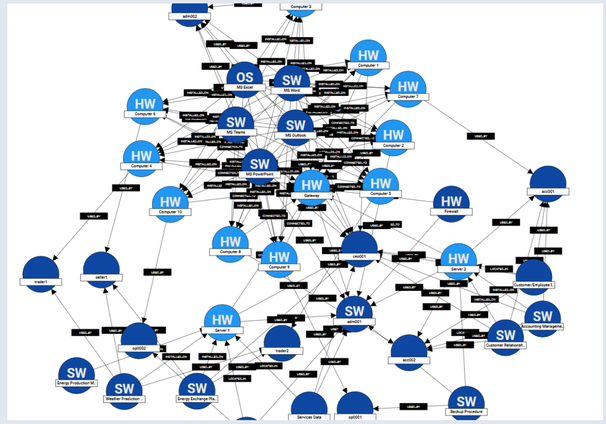
How will SECONDO use the Smart Contracts?

Smart contracts are self-executing programs with coded terms and conditions that automatically enforce and execute contractual agreements when predefined conditions are met. These contracts run on blockchain platforms and serve to automate and streamline various processes, eliminating the need for intermediaries. One of the defining features of smart contracts is their **autonomy**, as they operate without the necessity of a central authority. This autonomy is achieved by decentralized blockchain networks and consensus mechanisms. Another key feature is **immutability**, meaning once deployed, a smart contract's code cannot be altered, providing a high level of security and trust. Additionally, **transparency** is inherent in smart contracts, as their code and execution are visible on the blockchain for all participants to inspect. The **programmability** of smart contracts enables the creation of complex, self-executing agreements, ranging from simple transactions to sophisticated decentralized applications. While their potential for efficiency and automation is substantial, it's important to note that the technology is still evolving, and challenges such as security vulnerabilities and legal implications are areas that require ongoing attention and development.

SECONDO in the next Cyber Insurance Ecosystem

Blockchain technology stands poised to revolutionize the landscape of cyber insurance by introducing enhanced security, transparency, and efficiency to the industry. The immutability inherent in blockchain ensures the integrity of policy records and claims data, reducing the risk of fraudulent activities. The transparent and decentralized nature of blockchain enables all stakeholders, including insurers, policyholders, and regulators, to access a single version of trustworthy information, streamlining processes and minimizing disputes. Smart contracts automate claims processing, expediting settlements and providing a transparent mechanism for both insurers and policyholders. The technology's ability to create immutable audit trails proves invaluable in investigations, establishing a detailed and trustworthy history of events. Furthermore, blockchain facilitates secure data sharing for risk assessment and underwriting, allowing insurers to make more informed decisions. As blockchain evolves, its potential to reshape the cyber insurance landscape becomes increasingly evident, fostering a more resilient and trustworthy ecosystem.

Interconnection of assets in a business environment



The interconnection of assets in a business environment has a profound impact on cybersecurity risk, presenting a complex landscape of challenges. The expanded attack surface resulting from the integration of diverse devices and systems increases the likelihood of security breaches, with vulnerabilities in one asset potentially compromising the entire network. This interconnectedness also introduces the risk of chain reaction vulnerabilities, where the exploitation of one weakness can cascade through multiple assets. The sharing of sensitive data among interconnected components raises concerns about unauthorized access and data exposure. Dependencies on interconnected systems make the organization susceptible to disruptions in the event of a compromise, emphasizing the need for comprehensive security measures. The inherent complexity of managing interconnected environments demands continuous monitoring, timely patching, and a proactive cybersecurity posture.

Underwriting Cyber Risks
Risk Assessment
Policy Issuance
Incident Response Planning
Claims Management

Cybersecurity Audits
Coverage Limits
Premium Calculation
Data Breach Investigation
Regulatory Compliance

Implementing effective countermeasures is crucial to mitigating cybersecurity risks associated with the interconnection of assets in a business environment, and cyber insurance plays a vital role in this strategy. Organizations can bolster their defenses by conducting comprehensive risk assessments to identify vulnerabilities in interconnected systems. Cyber insurance policies tailored to the specific needs of the business environment can provide financial protection against potential losses resulting from data breaches, system compromises, and business interruptions. These policies often incentivize the implementation of robust cybersecurity measures by offering more favorable terms to organizations with proactive risk management practices. Network segmentation and continuous monitoring are countermeasures that help contain potential breaches and detect anomalies in interconnected assets. Employee training and awareness programs are essential components of a holistic cybersecurity strategy, as human error remains a significant threat. By investing in cyber insurance, organizations not only secure a financial safety net but also signal their commitment to proactive risk management, which can contribute to more favorable terms and coverage. In this interconnected landscape, cyber insurance serves as a valuable component of a comprehensive cybersecurity risk mitigation strategy.