Cloudscape2016
What the cloud and IoT mean for the digital single market

Title: How WISER is paving the ground for cyber security challenges in the DSM

Author(s): Elena González (ATOS), Antonio Álvarez (ATOS), Aljosa Pasic (ATOS)

www.cyberwiser.eu | @cyberwiser

Focus Area

Started in June 2015, the WISER Innovation Action will deliver, in late 2017, a cyber-risk management framework that dynamically assesses the cyber risk to which the client ICT infrastructure is exposed. This is done by continuously monitoring the risk associated to the cyber-climate of its ICT operational environment. It considers not only the technical side of cyber risk but also incorporates the business side, including socio-economic impact assessment. WISER builds on current state of the art methodologies and tools, leveraging best practices from multiple industries.

Given the traditional approach where cyber risk management is performed periodically, and the current state of art with risk management frameworks lacking an integrated, agile methodology to analyse cyber risks, a growing demand for the continuous monitoring of cyber security relevant events and the dynamic assessment of risk is more than evident.

The best answer about when a cyber attack threatens valuable assets calls for a reliable support for decision-making. WISER provides support to adopt the correct measures while maximising the return on Investment (RoI).

Who benefits and how?

Among the WISER goals, the highest priority is making cyber security affordable for SMEs.

WISER therefore mostly focuses on SMEs needs that often do not have means to handle cyber risks with advanced methodologies & tools, and cannot usually afford to hire a consultant. WISER will deliver a pre-packaged risk management solution for SMEs that combines a sophisticated solution with simplicity of use and adoption by the end-user.

On top of this, WISER is facilitating the uptake of a cyber-security culture that enhances business opportunities and competitiveness in the private sector, making cyber security a key selling point.

Digital Single Market Strategy

As the European Commission continues to progress its plans for a Digital Single Market (DSM), organisations across the region are beginning to think carefully about how their

initiative could impact them. Coupled with the impending adoption of the General Data Protection Regulation (GDPR), privacy and security issues are quickly moving to the top of the agendas of companies and policy makers.

The first step is to complete a cyber security and privacy assessment for the company´s cross-border business and digital services. Of course, an organisation cannot defend itself perfectly against every threat. Hence technology decisions need to be risk-based decisions. Thinking carefully about the size of the organisation and its appetite for risk, businesses should consider which areas are more vulnerable to threats, establish priorities for mitigation goals, and establish cost-efficient mitigation measures. It's important to understand that there is no one-size-fits-all standard for risk assessment: any successful evaluation has to be based on a thorough expert analysis leading to a comprehensive and holistic picture of the business risks.

WISER is aligned with the DSM, specifically with initiatives 12 and 13, contributing to increasing the cyber risk awareness by educating risk managers and boards of directors across the market.

To reach this new level in cyber security WISER will develop a methodology, based on best practices, with a set of taxonomies for cyber risk concepts, as well as a set of cyber risk checks and metrics.

The cyber risk framework will have to monitor the status of the ICT infrastructure cyber-climate not only at the ICT level itself, but also at the level of business processes and services running on top of these infrastructures. Furthermore, the business aspect also has a sociologicalal component also impacted by cyber risk. This is also evaluated, and is one of the main novelties brought by WISER.

WISER will provide decision support tools to facilitate selection of mitigation options based on dynamic risk evaluation, expressed in qualitative and quantitative terms, and integrating the tech, business and societal visions of risk. Focus is on integrating technological advances related to implementation of the continuous monitoring, assessment and mitigation mechanisms for cyber risk management in real time.

In conclusion, WISER represents advance over the state of the art by leveraging best practices today and recent research results. It is not simply about monitoring cyber incidents; it is about assessing the risk they mean to a company. It considers not only the damage to the ICT infrastructure, but also damage to the business, providing a multi-level assessment. This risk evaluation evolves as the cyber-climate changes. The definition of mitigation measures is assisted by the framework with solid criteria to apply to the decision-making. And all of this with a strong focus on SMEs with an aim to make cyber risk assessment and management affordable.