D8.2 – PRACTICAL TOOLS FOR ASSESSING THE SOCIO-ECONOMIC IMPACT OF RISK MANAGEMENT IMPLEMENTATION FOR CYBER SECURITY, FIRST VERSION

Work Package | WP8, Go to Market
---|---
Lead Author (Org) | Alberto Luca Biasibetti (AON)
Contributing Author(s) (Org) | Antonio Alvarez (ATOS), Alberto Luca Biasibetti, Sara Poidomani, Giorgio Aprile (AON) Roberto Cascella, Paolo Lombardi, Stephanie Parker, Fabio Gennai (TRUST-IT), Atle Refsdal (SINTEF), Roberto Mannella (REXEL)
Due Date | 30.11.2016
Date | 13.12.2016
Version | 1.0

Dissemination Level
- X PU: Public
- PP: Restricted to other programme participants (including the Commission)
- RE: Restricted to a group specified by the consortium (including the Commission)
- CO: Confidential, only for members of the consortium (including the Commission)
### Versioning and contribution history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>21.10.2016</td>
<td>Sara Poidomani (AON) and Alberto Luca Biasibetti (AON)</td>
<td>Table of Contents</td>
</tr>
<tr>
<td>0.2</td>
<td>24.10.2016</td>
<td>Sara Poidomani (AON) and Alberto Luca Biasibetti (AON)</td>
<td>Table of Contents updating</td>
</tr>
<tr>
<td>0.3</td>
<td>16.11.2016</td>
<td>Antonio Álvarez (ATOS)</td>
<td>Cost benefit analysis</td>
</tr>
<tr>
<td>0.4</td>
<td>16.11.2016</td>
<td>Sara Poidomani (AON), Alberto Luca Biasibetti (AON), Giorgio Aprile (AON)</td>
<td>First inputs on Section 2 and Section 3</td>
</tr>
<tr>
<td>0.5</td>
<td>16.11.2016</td>
<td>Roberto Cascella (Trust-IT), Paolo Lombardi (Trust-IT), Stephanie Parker (Trust-IT), Fabio Gennai (Trust-IT)</td>
<td>Socio-economic impact tool</td>
</tr>
<tr>
<td>0.6</td>
<td>17.11.2016</td>
<td>Alberto Luca Biasibetti (AON), Sara Poidomani (AON)</td>
<td>DEXi Model updating, inputs for Report’s rational output.</td>
</tr>
<tr>
<td>0.7</td>
<td>18.11.2016</td>
<td>Antonio Álvarez (ATOS)</td>
<td>Refinement on the section devoted to the cost-benefit analysis</td>
</tr>
<tr>
<td>0.8</td>
<td>25.11.2016</td>
<td>Atle Refsdal (SINTEF)</td>
<td>First Review</td>
</tr>
<tr>
<td>0.9</td>
<td>25.11.2016</td>
<td>Roberto Mannella (REXEL)</td>
<td>Edits following internal review</td>
</tr>
<tr>
<td>0.10</td>
<td>30.11.2016</td>
<td>Alberto Luca Biasibetti (AON), Sara Poidomani (AON) Roberto Cascella (Trust-IT), Paolo Lombardi (Trust-IT), Fabio Gennai (Trust-IT), Stephanie Parker (Trust-IT)</td>
<td>Addressing the issues from first review.</td>
</tr>
<tr>
<td>0.11</td>
<td>07.12.2016</td>
<td>Stephanie Parker, Roberto Cascella, Fabio Gennai (Trust-IT)</td>
<td>Further addressing issues from first review. Analysis of cyber risks and market positioning</td>
</tr>
<tr>
<td>0.12</td>
<td>07.12.2016</td>
<td>Atle Refsdal (SINTEF)</td>
<td>Second Review</td>
</tr>
<tr>
<td>0.13</td>
<td>07.12.2016</td>
<td>Alberto Luca Biasibetti (AON), Sara Poidomani (AON) Roberto Cascella (Trust-IT), Paolo Lombardi (Trust-IT), Fabio Gennai (Trust-IT), Stephanie Parker (Trust-IT)</td>
<td>Addressing the issues from second review.</td>
</tr>
<tr>
<td>0.14</td>
<td>09.12.2016</td>
<td>Roberto Mannella (REXEL)</td>
<td>Second review.</td>
</tr>
<tr>
<td>0.15</td>
<td>09.12.2016</td>
<td>Alberto Luca Biasibetti (AON), Sara Poidomani (AON)</td>
<td>Addressing the issues from second review and finalised executive summary.</td>
</tr>
<tr>
<td>0.16</td>
<td>12.12.2016</td>
<td>Antonio Álvarez (ATOS)</td>
<td>Version for General Assembly Approval</td>
</tr>
<tr>
<td>0.17</td>
<td>12.12.2016</td>
<td>Roberto Cascella (Trust-IT), Stephanie Parker (Trust-IT), Alberto Luca Biasibetti (AON)</td>
<td>Latest changes in Section 3.4</td>
</tr>
<tr>
<td>0.18</td>
<td>12.12.2016</td>
<td>Roberto Cascella (Trust-IT), Stephanie Parker</td>
<td>Additional changes in</td>
</tr>
</tbody>
</table>
D8.2 – Practical Tools for assessing the socio-economic impact of risk management implementation for cyber security, first version

Dissemination Level (PU)

www.cyberwiser.eu - @cyberwiser

<table>
<thead>
<tr>
<th></th>
<th>(Trust-IT), Alberto Luca Biasibetti (AON)</th>
<th>Section 3.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>13.12.2016</td>
<td>Antonio Álvarez (ATOS)</td>
</tr>
</tbody>
</table>

Disclaimer

This document contains information which is proprietary to the WISER Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to a third party, in whole or parts, except with the prior consent of the WISER Consortium.
Table of Contents

Executive Summary ................................................................. 1

1 Introduction ........................................................................... 2
  1.1 Purpose and Scope ........................................................... 2
  1.2 Structure of the document .................................................. 2

2 Socio-economic impact analysis and WISER Positioning .................. 3
  2.1 Analysis and positioning of WISER....................................... 4

3 WISER Socio-economic impact tool ........................................... 4
  3.1 Socio-economic input ......................................................... 5
  3.2 DEXi model .................................................................... 12
  3.3 Results ......................................................................... 12
  3.4 Report output ................................................................. 13

4 Cost benefit analysis ............................................................... 17
  4.1 Cost-benefit template and plans ......................................... 18

5 Conclusions and next steps ....................................................... 20

6 Bibliography ............................................................................ 20

List of Tables

Table 1: Socio-economic impact questionnaire ................................... 7
Table 2: Output of the questionnaire and rationale reported to the user ....... 16

List of Figures

Figure 1: Landing Page .............................................................. 6
Figure 2: Q0 Sector Information .................................................. 8
Figure 3: Economic Section ........................................................ 9
Figure 4: Sociological Section ..................................................... 10
Figure 5: Cyber Risk Management ............................................... 11
Figure 6: DEXi model evaluation tree ......................................... 12
Figure 7: Questionnaire Results .................................................. 13
Executive Summary

This document presents the first version of the socio-economic impact tool to provide a qualitative estimation of the socio-economic impact of cyber risk events in relation to the risk management of an organisation. One of the objectives of the socio-economic tool is to increase awareness of the consequences of cyber risks and encourage particularly small organisations (SMEs, small IT teams in public administration) to manage their risks more efficiently.

The tool is online at https://www.cyberwiser.eu/seit and it is provided for free and designed to be user-friendly. It serves as first demonstration of the benefits of using more advanced and complete WISER service, i.e. CyberWISER Plus, in cases where risk exposure and impact are both high to very high, by providing a more complex and complete estimation of the socio-economic impact of cyber risks.

The document first explains the rationale for the development of the tool. Then it provides the details of the design and implementation, including the DEXi model used to evaluate the socio-economic impact. For this first release, the document focuses on the socio-economic impact analysis as a foundation of the tool. As soon as a first set of respondents take the questionnaire, relevant case studies will be identified to map the socio-economic aspects of cyber risks on each one of the relevant sectors sharing results with peer projects. The analysis will be discussed in the next version of this document.

Additional features will be integrated in the final version of the socio-economic impact tool, which will be completed and finalised at the end of the project. As such, the deliverable also sets the roadmap for the integration of the functionalities identified, such as the cost-benefit analysis to offer a pragmatic view of how to mitigate efficiently (in terms of costs) potential socio-economic risks.
1 Introduction

This document presents the socio-economic impact tool to provide a qualitative estimation of the socio-economic impact of cyber risk events in relation to the risk management of an organisation. This is the first version of the tool, which will be completed and finalised by the end of the second year of the project (M24, May 2017). As such, the deliverable also sets the roadmap for the integration of the functionalities identified, such as the cost-benefit analysis to offer a pragmatic view of how to mitigate efficiently (in terms of costs) potential socio-economic risks.

One of the objectives of the socio-economic tool, as part of the work carried out in WP8 “Go to market”, is to increase awareness of the consequences of cyber risks and encourage particularly small organisations (SMEs, small IT teams in public administration) to manage their risks more efficiently. Being part of the WISER “light” approach, the tool is designed to be user-friendly and available as a free online tool. This tool also demonstrates the benefits of using more advanced and complete WISER service, i.e. CyberWISER Plus, in cases where risk exposure and impact are both high to very high, by providing a more complex and complete estimation of the socio-economic impact of cyber risks.

1.1 Purpose and Scope

Deliverable D8.2 is the first of two documents on the delivery of the socio-economic impact tool designed in relation to Task 8.5. The purpose of the task is to offer practical tools for assessing the direct and indirect impact of an organisation’s risk management implementation, prioritising business management responses with regard to equally important socio-economic impacts:

- **Economic impacts**, such as direct financial losses, business/time lost in dealing with the breach (including lost staff time), reduced market value, fines (e.g. also on the light of the forthcoming Network and Information Security Directive (NISD). These can be considered direct impacts.

- **Sociological impacts**, such as reputation damage, loss of market/customer confidence, growth potential, damage to the general public (e.g. theft of personal/sensitive data) and loss of IPR. These can be considered indirect impacts or knock-on effects across an organisation.

The tool is a simplified version of the cost-benefit analysis, fully integrated in CyberWISER-Plus.

It collects relevant statistics regarding the socio-economic impact of cyber risks for different market verticals based on questionnaire responses. In the second version of the tool, information will be anonymously aggregated, thus providing a significant benchmark that positions the organisation in its particular market vertical. The benchmark can therefore provide significant insights on socio-economic impact associated with specific market verticals.

In the WISER framework, the socio-economic impact tool leverages the DEXi [1] multi-decision qualitative model and analysis carried out in WP3 alongside the know-how acquired in WP2 for the development of the WISER services. With regard to the former, a simplified version of the DEXi model has been defined to qualitatively estimate the impact of cyber risk exposure, in terms of indirect and then direct impacts.

An updated version of the socio-economic tool will be released at the end of the second year (May 2017) and documented in Deliverable D8.3.

1.2 Structure of the document

The document follows the structure presented below:

- Section 1 introduces the document and its context as well as the structure of the document.
- Section 2 presents the socio-economic impact analysis as foundation of the tool.
- Section 3 describes the tool.
Section 4 presents the cost-benefit analysis that will be integrated in the second release of the tool.

Section 5 concludes the document and presents the next steps towards the release of the second version.

2 Socio-economic impact analysis and WISER Positioning

Cyber breaches are one of the most likely and most expensive threats to businesses. Yet few companies really understand how great their cyber risk exposure truly is, preventing them from effectively protecting themselves.

Losing valuable data can have a lasting impact on a company’s finances. Cyber security breaches affect businesses in all industry segments and the costs can be substantial. Financial costs may include reduced market value, reduced market share and fines. Many businesses are not aware of the costs of a cyber breach and are unable to make even the simplest estimation.

Impact is not only economic. It can also affect the customer base or supply chains, the ability to grow, and ultimately its reputation. Cyber attacks can hurt a company even if there is no gain for the perpetrator other than accessing sensitive information, causing reputation damage and reduced trust.

Reputation damage can undermine confidence of both customers and consumers in general, including lack of trust in information and communication technologies. Sensitive company data also needs adequate protection:

- Intellectual property, including new products and services stolen by third-parties.
- Supplier information.
- Employee details.
- Customer details.
- Accounts information.

Businesses need to be aware that protecting their company data not only helps secure their reputation but also puts the business in a stronger and more competitive position. Businesses therefore need to turn concerns about market competition into concrete actions. This is especially important for small businesses whose life may be highly dependent on IPR and/or the data they hold.

ICT hot spots, i.e., ICT clusters where small ICT tech firms are based, are currently among the most vulnerable but exposure changes rapidly in the evolving cyber space and as the number of digital businesses grows. For example, e-Commerce has become much more important to European businesses in recent years. In the UK, e-Commerce sales grew from £335 billion in 2008 to £573 billion in 2014 across non-micro businesses.

Yet most companies continue to misjudge which cyber security capabilities they should prioritise and often fail to obtain sufficient cyber security insurance protection. Moreover, small firms are less likely to seek external advice about cyber security than larger businesses. The UK Cyber Security Strategy 2016-2021 [2] (November 2016) highlights that the majority of businesses and individuals are still not properly managing cyber risks despite increased awareness.

It is essential that small businesses develop the capability to assess their cyber risk exposure and consequences from a socio-economic viewpoint. This is especially important for micro business owners that do not normally have IT specialists or cyber security staff. A practical approach to this dilemma is providing usable and useful tools to help businesses understand the nature and level of the threat they face, and guide them on how to best manage their own cyber security.

This is where WISER tools for SMEs come into play. CyberWISER Light is designed to give SMEs an understanding of the cyber risks, while the socio-economic assessment tool helps them quantify these risks. Evaluating a broader set of losses associated with cyber-attacks is key to fully understand the impact of a cyber attack, including perceptions of customers and the general public, reducing trust in...
the service being provided. (i.e. the direct users of the services provided by a company or indirect users via services supplied to third party companies).

The primary goal is to offer organisations a valuable estimation of the potential implications of their management of cyber risks from a socio-economic perspective. Sociological impact like reputation damage, may not be visible in the immediate aftermath of an attack but can harm the company. In the case of SMEs, reputation damage could even result in the complete closure of a business.

The secondary goal is to provide a free and online instrument to raise awareness of the potential risk of a cyber attack not only to the company assets, but also on the future business of the company that builds upon its reputation and trust of the end-users.

2.1 Analysis and positioning of WISER

WISER has dedicated effort in also lowering the entry barrier to cyber risk management for SMEs and small IT teams in the public sector. The aim is to demonstrate that cyber security does not have to be time consuming or complex. Several new tools follow the WISER “light” approach, such as CyberWISER Light and the Socio-economic Impact Assessment Tool, in enabling SMEs who are not IT or cyber-savvy to overcome time and financial constraints.

These WISER tools are complemented by awareness campaigns conducted in WP8, particularly helping companies recognise cyber security as a business performance issue or a good business practice, rather than simply an IT problem. WISER also promotes a staff culture that emphasises customer confidentiality and good data management. The Market Watch provides insights into the changing cyber risk landscape and promotes good practices and understanding of forthcoming EU regulations.

Such an approach responds well to key findings reported in the UK Cyber Security Strategy 2016-2021 [2] (November 2016) support the WISER “light” approach for small businesses and IT teams:

The market is not valuing, and therefore not managing cyber risk correctly. WISER tools lower the entry barrier to cyber risk management for SMEs and small IT teams. These tools also serve as a reality check to small organisations that hold commercially sensitive data on their IT systems and need adequate protection against cyber risks.

“Just under a fifth of businesses had their staff take part in cyber security training in the past year.” Cyber Security breach Survey 2016 [3]. Dedicated WISER tools facilitate understanding of cyber risks with tools that provide data and guidance that are actionable even for micro businesses.

“99.9% of exploited vulnerabilities were compromised more than a year after the vulnerability was published.” Verizon 2015 Breach investigation report [4]. WISER encourages continued self-assessment of risks and vulnerabilities by making its tools freely available online.

“Cyber security is key to unlocking innovation and expansion, and by adopting a tailored organisation and risk-centric approach to cyber security, organisations can refocus on opportunities and exploration” Ernst-Young Global Information Security Service 2015 [5]. This is the WISER approach for SMEs in a nutshell. The EU’s 20 million SMEs are increasingly becoming digital businesses in a hyperconnected world, where staying safe online will only grow in importance. CyberWISER Light and the Socio-economic impact tool are invaluable assets for these small businesses, helping them not only to assess and manage cyber risks but also to evaluate socio-economic impact on a regular and repeatable basis. Armed with valuable knowledge, SMEs can take the necessary actions.

3 WISER Socio-economic impact tool

As the socio-economic analysis involves assets that can sometimes be difficult to measure in terms of monetary values, such as reputation damage or reduced ability to grow, WISER offers a qualitative assessment usable by small organisations who lack cyber security experts within their team.

The socio-economic tool leverages the approach defined in WP3 and described in Deliverable D3.2 [6]. The process of evaluating the socio-economic impact of a cyber risk event starts with identifying qualitative criteria required to evaluate the sociological impact and the size/turnover of the company to
qualitatively forecast the potential economic impact. Then, the socio- and economic impacts are mapped with the organisation's processes for the management of cyber risks. This provides an organisation with a qualitative indication of the potential impact of cyber events at large and intelligence of the major causes.

A thorough analysis of the socio-economic impacts has been carried out in WP3 for the CyberWISER-Plus service. Work on this service highlights the value of a comprehensive framework that considers all aspects relevant to an accurate assessment of the cyber risk exposure and its potential socio-economic impact, requiring a large amount of information and preliminary analysis with specific support provided to the organisation. However, the design of a lighter version accessible to a larger audience, such as SMEs and small IT teams in public administration, can provide a first indication of the socio-economic impact, helping to define a more effective cyber security strategy. The result is an online tool that can be used as a Do-It-Yourself and completed in a few minutes without needing specific support from the WISER team.

3.1 Socio-economic input

The user-friendly online tool from WISER supports the calculation of the socio-economic impact of cyber risks. Users, whether SMEs or small IT teams, simply need to complete the online questionnaire, which addresses intangible, but very important, topics related to cyber risk. The questions are grouped into the following categories:

- **Statistical**: mapping the organisation with a specific industry sector. The purpose is to collect anonymous data to characterise each individual sector.

- **Economic**: identifying the size and annual turnover of the company, and what percentage relies on ICT technology to help understand the direct impact of a cyber security breach.

- **Sociological**: focusing on understanding and mapping the most important indirect or knock-on effects of a cyber security breach. Aspects considered here include not only reputation damage but lost business/staff time in responding to the breach, as well as damage to the general public. Other knock-on effects include loss of customer confidence or reduced ability to grow. In particular, WISER will consider how the reputation of an organisation could be impacted, and what would be the effect of cyber risks on company IPR. The general public may be affected by loss of personal or sensitive data) or may lose confidence in ICT-based solutions. Such data aims to trigger improved cyber security practices within small organisations and lead to more efficient cyber risk management.

- **Cyber risk management**: specifying the company processes to manage cyber security in order to contextualise the potential effects of a cyber attack, where greater awareness leads to direct actions taken.

The figure below shows the starting point for users of the tool.
Table 1 lists the 19 questions defined for the first version of the socio-economic impact tool, in addition to a first generic question indicating the industry sectors for statistical purposes. The questions have been defined by considering the nature of the tool: first indication of the socio-economic impact of cyber risks. As such, they have been conceived considering the most relevant aspects to base the assessment on, while ensuring that they are generic enough to cover a wide range of audience and organisation types.

<table>
<thead>
<tr>
<th>ID</th>
<th>Category</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q0</td>
<td>Statistic</td>
<td>What is your business sector?</td>
</tr>
<tr>
<td>Q1</td>
<td>Economic</td>
<td>What is your Company’s annual turnover?</td>
</tr>
</tbody>
</table>
Table 1: Socio-economic impact questionnaire

The first question (Q0) will not be used to compute the socio-economic impact, as such no qualitative value is associated and this is not an input for the model. However, the answer is utilized to identify the organization’s industry sector among well-defined categories, specified in the following figure.
The purpose of this question is to map the WISER socio-economic impact tool's user and characterise each industry sector by the potential socio-economic impact of cyber risks. This will provide an empirical indication of the cyber risk awareness per sector and a benchmark that can be used to position organisations. In order to have a statistical significance, this functionality will only be enabled as soon as a sufficient and significant number of respondents is reached.

The tool is configured to present to each user, upon authentication, the three categories on dedicated sections (see Figure 5).
Figure 3: Economic Section
Figure 4: Sociological Section
Figure 5: Cyber Risk Management

Users will be guided to answer the questions by providing examples for each one of the questions.
where a qualitative input is needed. Currently the tool presents only qualitative indications, but detailed choices will be specified in a subsequent release of the tool.

The results are presented in a report that can be downloaded by the user. The report indicates the societal and economic values and provides a justification of the qualitative score, including the main factors that contribute to the final assessment.

### 3.2 DEXi model

The socio-economic model for the tool is defined in DEXi. A thorough description of the DEXi language is available in Deliverable D3.2 [6]. Two (2) types of possible values are associated to the answers: Boolean value (yes/no), or qualitative value (very low, low, medium, high, or very-high). Figure 6 presents the DEXi tree used to evaluate the societal and economic impacts.

![DEXi model evaluation tree](image)

**Figure 6:** DEXi model evaluation tree

### 3.3 Results

The results are presented in a report that can be downloaded by the user. The report indicates the societal and economic value and provides a justification of the qualitative score, including what are the main factors that contribute to the final assessment. The report is presented in Figure 7.
3.4 Report output

The output, described at section 3.3, will present an overview to understand how Economical and Societal impact could be impact to the organisation. Otherwise, those two parameters are closely correlated to Cyber Risk Management.

<table>
<thead>
<tr>
<th>Section</th>
<th>Level Output</th>
<th>Rational</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economical</td>
<td>Very low</td>
<td>Your potential economic impact has a very low value, probably cyber incidents will not seriously affect your</td>
</tr>
</tbody>
</table>
business. Please consider that that security of your business might be impacted by the usage of new technology and relevant changes related to compliance and regulations for your sector.

<table>
<thead>
<tr>
<th>Dissemination Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>You are potentially vulnerable to a cyber attack that could be quite dangerous for your business. A risk management approach could help you to identify areas for improvement. An external assessment could provide indications on suitable approaches to implement, including countermeasures (both, technologies, processes and awareness) related to the business priority.</td>
</tr>
<tr>
<td>Medium</td>
<td>You could suffer a cyber attack that could be very dangerous for your business. Probably your IT security investments are ineffective and you should refine how to invest in security (both technologies and personnel). A good review of your IT Risk approach (or a new one) will be the first step to understand better the Cyber Risk and take the right approach and prioritise the use of new countermeasures into you environment.</td>
</tr>
<tr>
<td>High</td>
<td>A cyber attack has a very low impact for communities and citizen of your operating areas. However, it is important to not underestimate the consequence of a Cyber Attack that could compromise the operational of your organisation and have potential impact on the employees.</td>
</tr>
<tr>
<td>Very-high</td>
<td>A cyber attack could probably impact the community and the citizen interested by your area of operation. A cyber attack might not have a heavy return in terms of class actions or heavy brand reputation damage, but regulations and compliance could oblige you to do more effort to protect the society or community of your operating country.</td>
</tr>
<tr>
<td>Very-low</td>
<td>A cyber attack could have direct impact in terms of company reputation and personnel, and potentially profound impact on customers/citizens. As reported by “Ashley Madison” data breach (a worldwide data meeting website) [7], a cyber attack could affect the entire community, causing conflicts and reputational damages. This could lead to class actions against your organization if failing to properly protect your client’s data.</td>
</tr>
</tbody>
</table>

**Cyber Risk Management**

<table>
<thead>
<tr>
<th>Question</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q11¹</td>
<td>Based on IT Security Spending Trends - SANS Institute, for year 2015:</td>
</tr>
<tr>
<td></td>
<td>• About 29% of organisations spent between 0% and 3% of IT budget on Security purposes;</td>
</tr>
<tr>
<td></td>
<td>• About 17% of organisations spent between 4% and 6% of IT budget on Security purposes;</td>
</tr>
<tr>
<td></td>
<td>• About 12.5% of organisations spent between 7% and 9% of IT budget on Security purposes;</td>
</tr>
</tbody>
</table>

¹ Question number as reported in Table 1.
<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q12′</td>
<td>IT Security staff depends on several factors including the number of locations, the hardware and software used, the proficiency of users, and the hours of direct support. It’s difficult to pinpoint an exact number, but at least one responsible is needed to ensure adherence with security policies and best practices, and address the cyber threat.</td>
</tr>
<tr>
<td>Q13′ – Response</td>
<td>The risks to the organisation’s information assets from a cyber attack should be a regular agenda item for Board discussion. To ensure senior ownership and oversight, the risk of cyber attack should be documented in the corporate risk register and regularly reviewed; entering into knowledge sharing partnerships with other companies and law enforcement can help you in understanding new and emerging threats that might be a risk to your own business and also to share mitigations that might work. Based on UK Cyber Essential (“Reducing the Cyber Risk in 10 Critical Areas”) [8].</td>
</tr>
<tr>
<td>Q14′ – Response</td>
<td>A governance framework needs to be established that enables and supports a consistent and empowered approach to information risk management across the organisation, with ultimate responsibility for risk ownership residing at Board level. Third parties certifications can demonstrates your commitment to cyber risk management. Based on UK Cyber Essential (Reducing the Cyber Risk in 10 Critical Areas) [8].</td>
</tr>
<tr>
<td>Q15′ – Response</td>
<td>Consider the application of recognised sources of security management good practice, such as the ISO/IEC 27000 series of standards, and implement physical, personnel, procedural and technical measures. Based on UK Cyber Essential (Reducing the Cyber Risk in 10 Critical Areas) [8].</td>
</tr>
<tr>
<td>Q16′ – Response</td>
<td>Forty-nine percent of data breaches are caused by...</td>
</tr>
</tbody>
</table>
malicious or criminal attacks, and 19 percent are related to employee negligence. Based on the 2015 Cost of Data Breach Study by the Ponemon Institute. [9]

To address security threats, Companies have to arrange an integrated Risk Management process that includes the Cyber framework. This approach ensures the most effective method for an IT risk impact prevention/mitigation, thanks to the development of an appropriate awareness, while optimizing the process of transferring the risk to the insurance market. The insurance coverage of such risks is indeed the last step of a structured process that starts with the analysis of the specific company situation: From the type of business to the type of implemented activity, up to the IT infrastructure characteristics.

Based on “Italian Cybersecurity Report 2015 – A national Cybersecurity Framework” [10].

Cyber Insurance has to serve as a toll to protect the company balance, by covering the so called “catastrophic risks”, also based on the company risk appetite and risk tolerance. The Cyber policies could provide:

- **Defence Costs + Damages + Regulator Fines**
  Failure of Network Security, Failure to Protect / Wrongful Disclosure of Information, including employee information, Privacy or Security related regulator investigation, All of the above when committed by an outsourcer, Wrongful Collection of Information (some policies, Media content infringement / defamatory content)

- **Insured’s Loss**
  Network-related Business Interruption, Extra Expense, System Failure Business Interruption (some policies), Dependent Business Interruption (some policies), Intangible Asset damage)

- **Expenses Paid to Vendors**
  Crisis Management, Breach-related Legal Advice, Call Center, Credit Monitoring, Identity Monitoring, ID Theft Insurance, Cyber Extortion Payments

Table 2: Output of the questionnaire and rationale reported to the user

Table 2 outlines the content of the reported that will be presented to the user. Based on the assessment carried out from the sociological aspects linked with the cyber risk management of the organisation, the user will obtain as score (evaluated by using the DEXi model presented in section 3.2). An equivalent assessment will be computed for the answers to the economical part tool.

The user will also receive the evaluation of the cyber risk management of the organisation. The Socio-economic impact tool will output the implications of a missed management of the cyber risk within the organisation. The level of information is detailed in Table 2, where the corresponding rational will be presented to the users if the question has received a negative answer.
4 Cost benefit analysis

When it comes to putting in place appropriate countermeasures to cyber threats and actual cyber incidents, most companies fail to adequately understand the extent of a potential cyber breach, both in terms of direct and indirect impacts. There are several reasons for this:

- Cyber security is generally considered to be a technical problem rather than a business performance issue or as a good business practice based on a risk-assessment approach. Typically, staff culture does not emphasise customer confidentiality and good data management.
- Lack of key individuals in the organisation, particularly company boards, helping to champion cyber risk assessments and possible cyber insurance measures.
- Small firms are less likely to seek advice on cyber security practices, and according to the UK Cyber Security Strategy 2016-2021, have not yet started to use tools and services available to a sufficient extent despite greater awareness and high-profile media coverage.
- Most businesses do not have sufficient knowledge of the direct economic impacts of cyber risks nor of the indirect impacts due to risk exposure. Hence specific measures are not taken to mitigate such risks.

As a result, there is no support for the decision-making and the company’s managers end up taking decisions that have impact just in the short term, without any kind of underlying rationale justifying such decision.

Part of the WISER mission is to 1) increase awareness and promote actions to mitigate risks amongst the EU business community and 2) provide a dedicated tool that is usable and useful especially to small organisations (e.g. SMEs and small IT teams in public administration) lacking the skills and means for efficient risk management but facing a variety of potential impacts.

From a technical perspective, WISER addresses these challenges by incorporating a generic methodology in order to 1) propose mitigation measures addressed to specific cyber incidents and tailored to specific infrastructure elements; 2) analyse the convenience of applying it in the light of the costs and the benefits of the actual implementation. The former is being addressed in the context of modelling (WP3) activities. For the latter, this analysis serves two purposes: analyse the candidate countermeasure and, especially, compare it to other candidates. The cyber security budget is limited and the managers are interested in ensuring the maximum effectiveness of the countermeasure, thus an efficient cost benefit analysis helps companies, especially SMEs, to draw their own cyber security strategy.

WISER is an action-driven initiative, encouraging organisations to take a core set of steps towards better cyber risk management that effectively democratises cyber security (along the theme of “Cyber Security for All”). Customised reports generated by WISER SME tools, e.g. CyberWISER Light and the Socio-economic Impact Assessment Tool, gives organisations the information they need to make informed decision on cyber risk management.

WISER's innovative proposal in this respect encourages companies to establish a new culture where the cyber security decisions are made in an informed manner and after a deep analysis. This makes it possible to produce an outcome understandable from the managerial and business perspective, where the costs are broken down into relevant sections and the benefits are estimated.

While the calculation of costs, despite being estimations, can be done in a systematic way with a high degree of objectivity – to a certain extent based on the state of the art in cost estimation [11] – it is important to acknowledge that the estimation of the benefits is rather subjective. Historically, the financial benefits of cyber technology implementation have not been calculated with the same financial discipline used to evaluate other material investments. This was mainly due to a lack of readily available data and systematic methodology to support the efficacy of cyber investments. This gap has prevented managers from being able to formulate generally accepted financial metrics such as return of investment (ROI), net present value (NPV) and breakeven period, to communicate the value of cyber security projects and defend spending decisions [12].
concept of customer-perceived value (CPV) is used to emphasise the importance of customer’s perceptions on value [13]. Analogously, ‘perceived value’ can be used in security to emphasise the decision-makers perspectives.

Such value can be seen as the reduction of the risk in comparison to a scenario where no mitigation measures are in place. This is the intangible benefit, since investing on security measures is about avoiding risks, not about generating revenues. While there may be a general consensus on this definition, what seems really challenging is to get companies to agree upon a standard technique for calculating the internal cost of an incident.

With a focus on bringing some extra added value to the cost-benefit analysis tool, based on the aforementioned template, the Consortium does research on methods that help to ease the calculation of the benefits. A paper by Le Minh Sang Tran et al. [14] proposes to study how the likelihood and consequence of the risk is diminished as result of applying one or more mitigation measures. The paper also defines the thresholds of the levels of likelihood and consequence considered acceptable by the company, and pick the lowest cost combination of measures among those ensuring that likelihood and consequence levels are under the desired threshold. ENISA proposes, in a public paper [15], a method to calculate ROSI (Return of Security Investment) based on 3 variables: the estimated potential loss, estimated risk mitigation, and cost of the solution. A paper by Wes Sonnenreich [16] also mentions these variables and gives some hints on how to quantify them: measure the loss on intellectual property or the loss of productivity due to a downtime. Not only this, the paper mentions that it is also important to consider what may be the impact of the measure itself on the productivity. The author advises to focus on problems that are happening every day (email spam, bandwidth inefficiency, popup ads, installation of security patches...) rather than on major incidents less likely to happen. Another example can be found in the paper by Aora et al. [17], which shows a very illustrative example based on the scenario where an organization has to evaluate several components of its IT system in light of shrinking yearly operational budget. A very famous work that, despite being more than ten years old, still generates lots of discussions, is proposed by Gordon and Loeb. The dissertation is complex with advanced maths being involved, nevertheless it is worthwhile to remark the main finding saying that optimal expenditures do not always increase with the increase in vulnerability, and expenditures on security should almost never exceed 37% of potential loss [18]. Other techniques, like Monte-Carlo simulations, are proposed with a special focus on the banking sector [19].

These examples show that there are several proposals aiming at defining a more rigorous estimation of the benefits of investing on a certain security measure. As research goes on, some will be shown to be more accurate than others, but it is really unlikely to come up with a unique, universal, accurate and efficient methodology to provide these figures. What is actually paramount is to be correct when identifying independent and measurable factors, which are very relevant for the calculations to be done, and have a deep impact on the outcome. In other words, the consensus should be reached concerning: 1) the definition of ‘benefit of a mitigation measure’ and 2) the identification of the parameters to be used to estimate such benefit. If these two objectives are achieved, the methodology to be used is a matter of choice and experimentation.

As part of the socio-economic tool, WISER will make available a very early approach to present a template that can be filled out by the user in order to estimate the costs and the benefits of implementing certain mitigation measures. This service will be offered for free as a teaser of what will be provided in CyberWISER-Plus, which features a more detailed template (see deliverable D5.2 [20]), with the support provided by the WISER experts. The user will be able to play with the template and compare two different mitigation measures. In order to help the user, WISER will point to the documentation referred to in this deliverable and will encourage the users to analyse it thoroughly in order for them to find their own way to approach the challenge. More details are presented in Section 4.1.

### 4.1 Cost-benefit template and plans

The template that will be presented to the user in order to obtain information to carry out a cost-benefit analysis will be composed of the following sections:
1) **Investment costs:** this section covers the initial investment that has to be done to put in place the corresponding mitigation measure.
   a. **Management personnel** deals with the costs that managerial positions will incur related to making the mitigation measure available.
   b. **Tech personnel** addresses the costs that technical positions will incur related to making the mitigation measure available.
   c. **Equipment purchase** is related to the costs that will involve acquiring the needed equipment to apply the mitigation measure, if any.
   d. **Software purchase** concerns the costs of acquiring any software needed to run the mitigation measure, if any.

2) **Future costs:** this section invites the user to reflect the cost that will incur keeping the mitigation measure available for a certain timeframe.
   a. **Management personnel** indicates costs related to managerial positions for the defined timeframe.
   b. **Tech personnel** deals with the costs related to the technical profiles for the defined timeframe.
   c. **Equipment updates** indicates the costs concerning keeping the equipment up to date, in order to apply correctly the mitigation measure.
   d. **Software updates** refers to the costs to keep the software up to date, in order to apply correctly the mitigation measure.

3) **Future benefits:** this section addresses the estimated benefits, for a certain timeframe, of applying the mitigation measure.
   a. **Reduction of damages.** The user is asked to estimate to which extent, in terms of money, the damage to company digital assets will be reduced as a consequence of applying the measure.
   b. **Reduction of operational costs / resources.** Any incident involves extra expenditure on operational costs and resources to fix the problem occurred. A clear benefit of putting in place a mitigation measure, thus diminishing the likelihood of the incident, would be to reduce those potential expenditures, that would be seen as a benefit of the measure.
   c. **Reduction of insurance fees.** If the company has contracted an insurance for cyber incidents and incidents materialize, it is expected that the insurance premium gets more expensive for the company. On the contrary, preventing incidents means keeping the insurance premium at its level or even managing to lower it. This can be seen as a clear future benefit.

The result of the analysis will be a comparison of:
- The total costs (investment + maintenance).
- The total future benefits.
- The investment margin (benefits – costs).
- The ROSI (Return of Security Investment): (benefits – costs) / costs. The mitigation measure having a positive ROSI is worth to be applied. The measure with the highest ROSI would be the one providing the maximum value for money.

WISER provides the template for the cost-benefit analysis but will not support any particular approach to obtain the figures with which the template is filled. However, WISER will make available documentation resources describing different approaches to the problem (e.g., the documents referred to in this deliverable will be linked on cyberwiser.eu). Additional research efforts will be made in the
coming months to expand this library of resources oriented to enlighten the user in the process of establishing a framework for the decision-making process.

5 Conclusions and next steps

This deliverable describes the socio-economic impact tool. First it explains the rationale for the development of the tool. Then it provides the details of the design and implementation, including the DEXi model used to evaluate the socio-economic impact. The document describes the tool itself, which should be considered the real focus of the deliverable.

The tool will be refined in the coming months to include additional features (e.g. the positioning of the organisations with respect to their industry sector). The tool will also integrate the cost-benefit analysis, that has been duly reported at this stage in this document.

The roadmap to follow will be the following:

- February 2017:
  - Initial version of the free cost-benefit analysis tool available for cyberwiser.eu users.
  - Initial set of documents enlightening the process of obtaining the figures with which the cost-benefit template is filled.

- April 2017:
  - Refined version of the free cost-benefit analysis tool available for cyberwiser.eu users
  - Expanded set of documents enlightening the process of obtaining the figures with which the cost-benefit template is filled.
  - Initial collection of practical case studies to illustrate the users with.

- November 2017
  - Final conclusions on cost-benefit methods research and case studies. This will include the feedback from a public workshop to be held during the final year of the project.

The tool is available online at [https://www.cyberwiser.eu/seit](https://www.cyberwiser.eu/seit). As soon as a first set of respondents take the questionnaire, relevant case studies will be identified to map the socio-economic aspects of cyber risks on each one of the relevant sectors sharing results with peer projects. The analysis, which will be combined with the assessment of the Wiser Early Assessment Pilots, will be discussed in the next version of this document.

6 Bibliography


2015-7?r=US&IR=T


[17] Dennis Hall, C. Ariel Pinto, Dwayne Ramsey, and Rahul Telang Ashish Arora, "An ounce of prevention vs. a pound of cure: how can we measure the value of IT Security solutions?," Berkeley, California. UNT Digital Library.,

