cyberwatching.eu
The European watch on cybersecurity & privacy

cyberwatching.eu CYBER RISK TOOL

Cyberwatching.eu Initiative: Cyber Risk Temperature Tool

Insights and recommendations from Cyberwatching.eu

2021

cyberwatching.eu consortium

Trust-IT Services
Communicating ICT to markets

Oxford e-Research Centre

University of Oxford

ICT Legal Consulting
Balboni Bolognini & Partners

European Digital SME Alliance

CONCEPTIVITY

360 SECURITY

AON

aeiciberseguridad
Agrupación Empresarial Innovadora CIBERSEGURIDAD y Tecnologías Avanzadas

Table of content

List of tables

List of figures

Disclaimer

The work described in this document has been conducted within the project cyberwatching.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under Grant Agreement no.740129. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

1 Introduction

In view of the updated EU Regulations requirements as explained in Chapter 2 of D3.5 Risk and recommendations on cybersecurity services[1], followed by the challenges in emerging technologies as explained in Chapter 3 of D3.5, cyberwatching.eu initiated the creation of **a tool to assist SMEs in understanding the real situation about their cyber security environment**. The main objective of this tool is, therefore, to provide SMEs with a preliminary assessment of its cyber security readiness in a cost-effective manner. By means of a short but complete questionnaire, an SME may obtain a preliminary evaluation of its cyber security readiness in a cost-effective manner and thereby, consider undertaking actions that would be necessary in order to enable it to become more resilient. Ideally, the questionnaire should be completed by the person with the most technical skills within the company. The full questionnaire is provided in Annex 2.

2 Structure of the Questionnaire

The questionnaire consists of two main parts. In the first part, the respondent is asked to provide a personal assessment of the IT level of security within the company. In the second part, the respondent is asked questions of a more specific and technical nature. Through the attribution of a score, the SME is placed in one of the following profiles (in the order of *severity*):

- Low vulnerability;
- medium-low vulnerability;
- medium-high vulnerability;
- high vulnerability.

Thus, the evaluation is performed through a set of questions that are based on the need to analyse the company through different areas, such as:

- Specific knowledge of the cyber security readiness within the company;
- the methodologies followed within the company;
- the distribution of administrative fees on the systems;
- the information segmentation policy;
- authentication policies for access to corporate systems;
- other assessments previously carried out.

The afore-mentioned topics were selected because they were considered as the starting point and as essential for a careful analysis in terms of cyber security.

[1] https://cyberwatching.eu/d35-risk-and-recommendations-cybersecurity-services

3 Methodology

As mentioned above, the interviewee is required to complete a questionnaire consisting of **two distinct parts**: the first part represents a **self-assessment** evaluating the cyber-risk vulnerability rate of the company, whereas the second part, based on few questions, seeks the **real data regarding that very rate**.

More specifically, the first three questions work on a rating system: the interviewee is required to provide a self-evaluation with a rating from 1 to 7, where 1 indicates the lowest value and 7 the highest.

For each answer:

- 4 points are assigned to interviewees who provided the values 1, 2 or 3;
- 8 points are assigned to those who provided the value 4;
- 16 to those who select 5;
- 20 points are assigned to the values 6 and 7.

The second part of the questionnaire consists of eleven questions, including some sub-questions, which represent a real and objective evaluation. In these cases, just one option is provided:

- for each answer, a value from 0 to 10 is assigned,
- rating the possible options from the best to the worst.
- In a particular situation, 15 is the value assigned to answers which reflect a notably severe situation.

Once the questions are completed, the tool calculates the final score, which is obtained by averaging the scores of each question in both parts of the questionnaire.

4 Explanation of Scores

For the **first part** of the questionnaire, four scoring ranges have been created, and for convenience **are numbered from 1 to 4**, where 1 indicates low confidence in one's computer security (1- |6) and 4 indicates high confidence in one's computer security (18- |20).:

Self-assessment	
Low confidence in your IT security (1-6),	1
Medium-low confidence (6-12),	2
Medium-high confidence (12-18),	3
High confidence (18-20).	4

Table 1: Cyber Risk Temperature Tool – Self-assessment score

The definition "*Confidence in own cyber security"* means how the respondent assesses their cyber security readiness. This is important because each person takes decisions regarding cyber security issues based on his or her individual assessment of corporate cyber security.

Although this is important, it does not mean anything on its own. It is included in a matrix with the results obtained from the answers to the questions in the **second part** (average of the scores obtained), also divided into 4 ranges:

Rating	
Low vulnerability (0 ≤ M ≤ 3),	1
Medium-low vulnerability (3 ≤ M ≤5),	2

Medium-high vulnerability (5 < M ≤ 7),	3
High vulnerability (7 < M ≤ 12).	4

Table 2: Cyber Risk Temperature Tool - Rating score

When crossing the two axes, the matrix returns a scale from -3 to 3.

		Rating			
		1	2	3	4
Self-assessment	1	-3	-2	-1	0
	2	-2	-1	0	1
	3	-1	0	1	2
	4	0	1	2	3

Table 3: Self-Assessment Matrix

The returned scale from the matrix indicates the coherence between the subjective evaluation of the respondent and the objective evaluation of the company, an indicator of the **perception of the company's cyber security.**

Very under-estimated	Under-estimated	Slightly under-estimated	Consistent with self-assessment	Slightly over-estimated	Over-estimated	Very over-estimated
-3	-2	-1	0	1	2	3

Table 4: Indicator of company's cyber security

5 Explanation of Results

While evaluating the vulnerability rate, the perception must be considered as an added factor.

The tool will return the description of **the vulnerability range and in addition the value of perception**. The possible combinations that can be obtained are the following:

Profile 1[2]: Congratulations, your company has **Low vulnerability** and your perception of cyber security […][3] The real situation:

> As a result of the carried-out assessments, your company has proved that it fulfils the main requirements demanded for adequate cyber security. You are recommended to keep updated on cyber security issues at all times.

Profile 2: Your company has **Medium-low vulnerability** and your perception of cyber security [...] The real situation:

> As a result of the assessments carried out, your company only partially meets the main requirements for adequate cyber security. You are recommended to keep updated on cyber security issues and consider contacting a cyber security expert for a more in-depth evaluation.

[2] Temporary name

[3] It is the value of your company's cyber security perception

Profile 3: Attention! Your company has **Medium-high vulnerability** and your perception of cyber security [...] The real situation:

> As a result of the assessments carried out, your company does not meet most of the main requirements for adequate cyber security. You are recommended to contact an expert in the field who can provide you with adequate support to identify and mitigate the vulnerability.

Profile 4: Attention! Your company has **High vulnerability** and your perception of cyber security [...] The real situation:

> As a result of the assessments carried out, your company does not meet the main requirements for adequate cyber security. You are strongly recommended to urgently contact an expert in the field to mitigate your numerous vulnerabilities.

6 Testing and launch campaign

The Cyber Risk Temperature Tool was developed and implemented in August 2020.
Before the official launch in October 2020, an internal testing phase was launched among the Consortium to spot possible bugs and improvements.

The launch of the tool was accompanied by a promotional campaign which included the following:

- Landing page set up
- Promotion to Concertation mailing list (93 members)
- Social media promotion
- Newsletter to the cyberwatching.eu community (> 1000 members)

Another promotional campaign was launched in January 2021 (and is currently ongoing) with the help of the whole Consortium including a promotional article to be published on external sources and social media posts and images ready to be shared.

7 Analysis of results

As of now, the Cyber Risk Temperature Tool gathered 26 responses coming from the following countries:

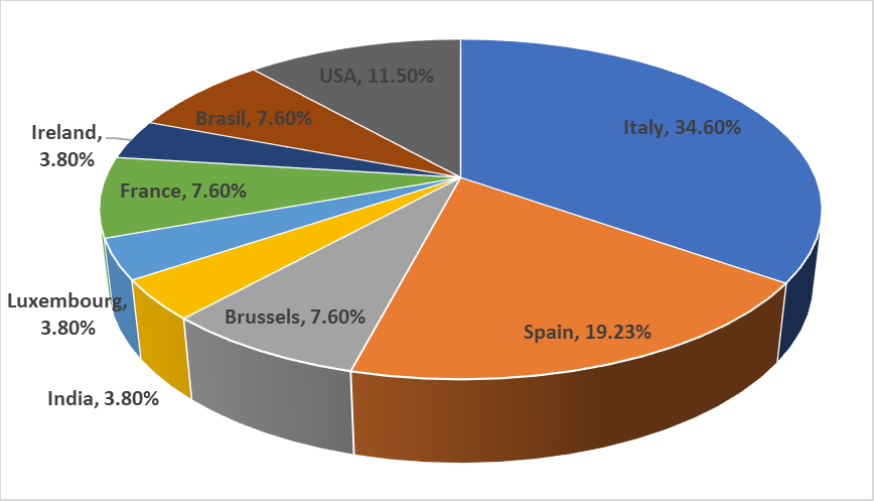

Figure 1: Cyber Risk Temperature Tool - Country breakdown

By analysing in depth, the responses of the questionnaires, the results show that the perception of companies concerning their cybersecurity assessment is for the vast majority that they are in a very good position with low vulnerabilities indicated, with 50% of companies indicating a slight underestimation and 26.6% indicating a perception in line with the assessment

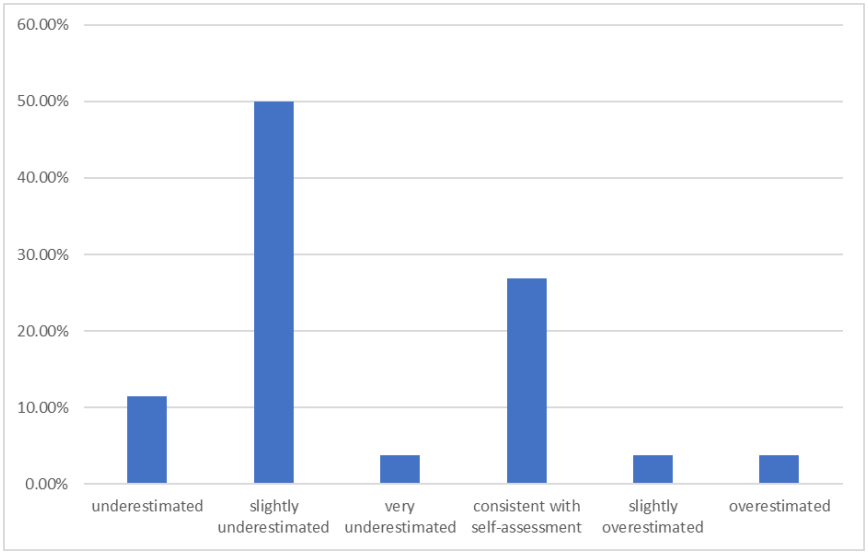

Figure 2: Cybersecurity perception analysis

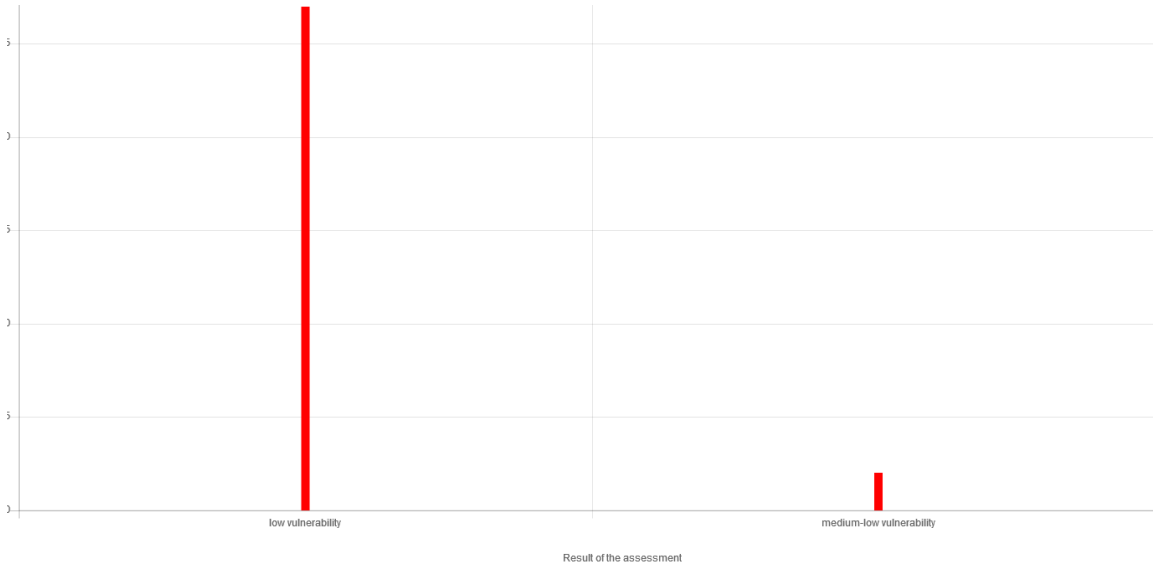

Figure 3: Cybersecurity vulnerability perception analysis

These findings are also backed up by the fact that the majority of respondents have a firewall in place to protect their devices and that they perform back-up of their data either every day (38%) or every week (18%).

It is important to note that 38% respondents indicated that their company is following best practices or frameworks (e.g., OWASP, NIST and COBIT) and also regularly carrying out training courses about cybersecurity.

8 Related Cyberwatching.eu Publications

- Cybersecurity risk management: How to strengthen resilience and adapt in 2021[4]
- Building STRONG CYBERSECURITY in the European Union[5]
- EU Cybersecurity legal and policy aspects: preliminary recommendations and road ahead[6]
- European Cybersecurity and Privacy Research and Innovation Ecosystem[7]
- Cybersecurity and Privacy ecosystem model report[8]

[4] https://cyberwatching.eu/publications/cybersecurity-risk-management-how-strengthen-resilience-and-adapt-2021
[5] https://cyberwatching.eu/publications/building-strong-cybersecurity-european-union
[6] https://cyberwatching.eu/publications/eu-cybersecurity-legal-and-policy-aspects-preliminary-recommendations-and-road-ahead
[7] https://cyberwatching.eu/publications/european-cybersecurity-and-privacy-research-innovation-ecosystem
[8] https://cyberwatching.eu/publications/cybersecurity-and-privacy-ecosystem-model-report

cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740129.