A Work Project, presented as part of the requirements for the Award of a Master's degree in Management from the Nova School of Business and Economics.

# CONSULTING PROJECT WITH THE TOPIC: "AGEAS CONSULTING FIELD LAB ON A CYBER RISK VALUE PROPOSITION"

AFONSO CARVALHO GOMES | 29032

MADALENA MADEIRA SANGALHO | 29203

RAQUEL DE MACHADO NETO E SANTOS BRITES | 29212

Work Project carried out under the supervision of:

Professor Constança Monteiro Casquinho

04.01.2021

# Abstract

The project focuses on the strategic assessment of the potential value for insurers in cyber risk and the development of a comprehensive and successful value proposition for Ageas in this market. To fulfil these objectives, external and internal analyses were conducted, to identify opportunities and threats of the cyber insurance market and Ageas' strengths and challenges to enter in it. Afterwards, profitability indicators (market size and claims ratio) were measured to understand the potential for Ageas in this market. The team proceeded by formulating hypotheses and testing them through industry experts' interviews, customer in-depth interviews and surveys. The outcome of this project is a set of recommendations grounded on the five pillars of an efficient value proposition – target segments, product (coverage, type and structure), "go-to-market" plan, underwriting solutions and a pricing concept – for B2B and B2C.

**Keywords:** Ageas, Cyber Risk, CyberShield, Value Proposition, Market Size, Claims Ratio, Target Segments, Product, Engagement, B2B, B2C, Underwriting Challenges, Pricing Concept

This work used infrastructure and resources funded by Fundação para a Ciência e a Tecnologia (UID/ECO/00124/2013, UID/ECO/00124/2019 and Social Sciences DataLab, Project 22209), POR Lisboa (LISBOA-01-0145-FEDER-007722 and Social Sciences DataLab, Project 22209) and POR Norte (Social Sciences DataLab, Project 22209).

# Acknowledgments

We would like to express our very great appreciation and gratitude to Professor Constança Casquinho, for her indispensable orientation and guidance throughout the project. The willingness of Professor Constança to generously and tirelessly give her time to supervise, assist and advise us with her valuable suggestions and positivity have enabled us to grow not only as consultants but also at a personal level.

We are also undoubtedly thankful to Dr. Nelson Azevedo, for his availability and orientation during the project. His great expertise as well as constructive insights helped us convert our analysis into actions, in the most efficient way. Furthermore, for all the constant encouragement, availability and feedback, we would also like to express our appreciation to Dr. Diogo Paiva and Dr. José Barreiros, whose industry expertise and pragmatic orientation assured our deliverables were aligned with the client’s expectations. Moreover, the team is also thankful to Dr. Luís Lima whose active support and assistance, in the last two months, were crucial to the development of the project. Lastly, to all, we would like to thank for the warm welcome in Ageas Portugal and for making us feel part of the team.

Additionally, the team would like to express their gratitude to Dr. Katrien Buys, Dr. Eduardo Caria and Dr. Rauf Gucuk for their expert guidance and fruitful feedback and for their availability and attention in hearing our analysis and recommendations, fostering our motivation and learning.

To all the aforementioned, as well as our professors and colleagues from Nova School of Business & Economics, thank you for the personal and academic knowledge that made our learning curves steeper.

Lastly, we would like to express our deep gratitude for the endless support and encouragement of our friends and families, particularly our parents, who made it possible for us to live in a world of possibilities.

# Consulting Labs aim to assist companies in solving real business and strategy challenges, generating a win-win outcome for both parties – Ageas Portugal Group and Nova SBE Team – based on a trusted relationship.

## Ageas Consulting Lab

- Ageas Portugal Group benefits from **high-quality** problem identification, structuring and solving and capitalize on a great **investment-quality relationship.**
- Have a **structured** and **highly disciplined** approach from a team with **great analytical**, **creative** and **learning** capacity.
- Strengthen the relationship with the University – privileged access to a **highly-skilled recruitment supply** and **connections with academic experts** from diverse areas.


*Figure 1: Exchange between Ageas Portugal and Nova SBE*

- The team from Nova SBE benefits from **active participation in** a **real** and **practical** consulting project.
- Apply **theoretical knowledge** acquired throughout the academic career.
- **Collaborate** and **learn** cross-sectional work **methodologies** from an international Insurance Group.
- **Develop** several **soft** and **hard skills**, namely analytical, communication, team-work and time-management.

# Glossary

| Word | Definition |
| --- | --- |
| ASF | Autoridade de Supervisão de Seguros e Fundos de Pensões |
| Avg. | Average |
| Beyond Insurance | Ongoing relationship with the client without necessarily having a claim |
| B2B | Business-to-business |
| B2C | Business-to-consumer |
| BP | Best Practice |
| CAGR | Compounded Average Growth Rate |
| CEJ | Customer Experience Journey |
| CEO | Chief Executive Officer |
| CTO | Chief Technology Officer |
| CRM | Customer Relationship Management |
| DSP | Digital Service Provider |
| E.g. | For example |
| EU | European Union |
| GDP | Gross Domestic Product |
| ICT | Information and Communication Technology |
| InsurTechs | Combination of the words “insurance” and “tech”, used to define innovative technologies and new digital tools to optimize the performance of insurance companies |

| Word | Definition |
| --- | --- |
| ISACs | Information Sharing and Analysis Centres |
| IT | Information Technology |
| MECE | Mutually Exclusive, Collectively Exhaustive |
| MI | Management Information |
| Min | Minutes |
| MRM | Model Risk Management |
| No. | Number |
| PoD | Points of Differentiation |
| PoP | Points of Parity |
| Q&A | Questions and Answers |
| RDS | Realistic Disaster Scenario |
| OES | Operator of Essential Services |
| OPEX | Operational Expenditure |
| OT | Operational Technology |
| SCQA | Situation Complication Question Answer Framework |
| Syndication | Continuously working in partnership with the client |
| SME | Small and Medium Enterprises |
| STP | Segmentation, Targeting, Positioning |
| USA | United States of America |
| WTB | Willingness to Buy |
| WTP | Willingness to Pay |

*Table 1: Glossary*

# Agenda

# Executive Summary

**Methodology** – The master thesis consisted of a consulting lab in collaboration with Ageas Portugal. The Pyramid Principle introduced the project's overriding question "Should Ageas enter the cyber insurance market?" addressed in four phases – diagnosis, analysis, strategy formulation and recommendations. The deductive reasoning emerged from the external and internal analyses conducted through six frameworks (PESTL, Porter's Five Forces, Industry Life Cycle, Resource Based View, Porter's Value Chain and SWOT & TOWS), competition analysis and forecast of profitability indicators. Porter's Generic Competitive Strategies, STP Model and 7Ps Marketing Mix underpinned the inductive reasoning; the team resorted to various sources – internal company and secondary data, industry experts and in-depth interviews and surveys. **Diagnosis** – Ageas is a multinational insurance group with a diverse portfolio that goes beyond insurance. A cyber policy is typically composed of pre-breach services and general coverage. **External Analysis** – The escalation of cybercrime allied to technological advances favor the cyber insurance industry, currently in its growth stage. The forecasted market size indicates great potential, the claims and loss ratios confirm the industry's profitability and thus, a rising rivalry is expected. **Internal Analysis** – Ageas will leverage on its strong reputation (supported by a customer centric, technology-driven culture) to tackle main threats (e.g., complex underwriting), to overcome challenges (e.g., scarcity of data) – to ultimately exploit opportunities. **Strategy Formulation** – Differentiation strategy should guide Ageas' strategic decisions. Leveraging on survey's insights, the team segmented and profiled customers and proposed Ageas to follow differentiated marketing to SMEs and families. The positioning will focus on exploring untapped demand to "deliver an emotional and meaningful experience", while controlling claims and risks. **Recommendations** – Ageas should develop two value propositions – (1) for SMEs and (2) for families – with multiple plans and optional modules differentiated by targeted employee training (for SMEs) and online protection (for families). It should design a customer-centric "go-to-market" plan to place CyberShield in the most suitable brands and distribution channels, to develop awareness and engagement strategies and to empower the salesforce. The implementation of underwriting solutions and the design of an appropriate pricing concept enables the delivery of comprehensive, transparent and tailored solutions at an adequate price. The action plan comprises 5 steps and culminates in the launch of CyberShield, predicted for July 2022. The main challenges faced throughout the project were the scarcity of available data and the complexity of the proposed topic – cyber insurance.

# Relevant theories, frameworks and models were described in the literature review, to efficiently develop an overview of the project's methodology.

B

## B.1. Methodology | Literature Review (I/II)

To tackle consulting projects, teams must adopt McKinsey's problem-solving methodology popularized by Minto, B. (1985) as **"The Pyramid Principle"** to ensure structured reasoning and clear communication with the client. Therefore, the top-down approach starts by answering the project's overriding question – resultant from the **SCQA framework** – followed by its breakdown into MECE arguments and supporting facts – compiled in an **issue tree.** Hence, **deductive reasoning** is applied through an external and internal analysis to validate the overruling message; while **inductive reasoning** is developed by formulating well-informed hypotheses – tested in the **fact-pack** stage – on how to address the project's challenge.

Firstly, to comprehend the external and macro environment, a **PESTL analysis** should be applied to understand the Political, Economical, Social, Technological and Legal forces surrounding the business ecosystem. This framework, firstly mentioned as ETPS by Aguilar, F. J. (1967), shows how the main opportunities and challenges led by the aforementioned forces affect the business. Furthermore, a **Porter's Five Forces** analysis, firstly used by Porter, M. (1979), should be performed to assess the micro environment. This framework evaluates the effect of the collective strength of competitive forces in the industry's profitability and how the company can defend itself from these forces or use them in its favour. Finally, a **Product Life Cycle** analysis, developed by Vernon, R. (1966) should be followed, in order to characterize strategic topics corresponding to different stages of an industry's development. To better understand the cybersecurity field, as well as the behaviours and perceptions of potential customers' towards the offer, **qualitative and quantitative research methods**, should be performed. Therefore, **expert interviews** should be executed to gather knowledge on cybersecurity, since, as asserted by Meuser M. and Nagel, U. (2009), they are a **qualitative research method** that allows expert knowledge on a specific field. Moreover, to gather descriptive data on customers' perceptions and thoughts about the product, **in-depth interviews** should be conducted, according to Malhotra, N. K., Nunan D. and Birks, D. F. (2017). Finally, to collect statistically significant information about potential customers' needs and preferences, **quantitative research methods** should be taken.

# Relevant theories, frameworks and models were described in the literature review, to efficiently develop an overview of the project's methodology.

B

## B.1. Methodology | Literature Review (II/II)

To start understanding the internal environment, the **Value Chain framework** developed by Porter, M. (1985) must be applied to assess the company's value creation, i.e., the process of delivering valuable services to its final customers. Hence, according to Cristopher, M. (1992), primary and support activities' organization and performance are examined to disclose key elements deriving competitive strategy. Further on, according to Barney J. (1992), the **Resource-based View Model** must be applied to identify a firm's resources – assets, capabilities & competencies – that fulfil the VRIO criteria – and thus, have the potential to deliver sustainable competitive advantage. Nevertheless, all the resources and activities should not be neglected, as they are indispensable for the company's functioning and success.

Having assessed the internal context (company's activities and resources) and the inherent external environment (macro and micro context) it is crucial to compile all these insights in a **SWOT analysis** – created by Humphrey, A. (1960) – to highlight how to leverage on firm's strengths and weakness to take advantage of the external opportunities and threats. The next step is to perform a **TOWS analysis** – correlates the four dimensions – to reduce threats, enhance strengths, exploit opportunities and eliminate weaknesses. The ultimate objective is to transform the SWOT findings into future strategic options.

According to Porter, M. (1980), after an integrated analysis, a firm must select the right **generic competitive strategy** – cost leadership, differentiation or focus – to avoid the "stuck in the middle scenario", where it is not able to retain a sustainable competitive advantage. Leveraging on consumer insights – from the aforementioned qualitative and quantitative methods – and guided by the overall strategy, the firm can follow Kotler, P. & Keller, K. (2005) **STP Model**. It identifies and profiles potential customers (segmentation), assesses attractiveness and selects which segments to pursue (targeting), and formulates the value proposition and action plan (positioning). To deliver the former, it is crucial to construct a **marketing mix** grounded on **7Ps** (Product, Promotion, Place, Price, People, Process and Physical Evidence) – Booms, B. and Bitner, M. (1981). Finally, an action plan acts as a roadmap to implement the set of recommendations, clarifying the main tasks, steps, responsibilities and timeline to achieve the ultimate goal – the launch of Ageas CyberShield.

# The definition of collaboration goals and the scope of the project was crucial for the alignment of expectations with Ageas. The schedule of weekly and steering meetings allowed for constant feedback throughout the project.

## B.2.1. Methodology | Project Methodology – Collaboration Goals, Timeline and Scope

**COLLABORATION GOALS & TIMELINE**

| A. Strategic assessment of the potential value for Insurers in cyber risk | September | | | | October | | | |
|---|---|---|---|---|---|---|---|---|
| | 7 | 14 | 21 | 28 | 5 | 12 | 19 | 26 |
| • Assess overall cyber insurance market situation | | | | | | | | |
| • Benchmark and Best-Practices Analysis | | | | | | | | |
| • Evaluate client's awareness, exposure & willingness to adopt cyber insurance | | | | | | | | |
| • Identify mismatch between client's needs and insurers offers | | | | | | | | |
| • Quantify market size (current & potential) – serviceable and obtainable | | | | | | | | |

| B. Development of a comprehensive and successful value proposition | November | | | | | December | | |
|---|---|---|---|---|---|---|---|---|
| | 2 | 9 | 16 | 23 | 30 | 7 | 14 | 21 |
| • Target customer clusters | | | | | | | | |
| • Structure cyber product – coverages and benefits | | | | | | | | |
| • Frame the product within Ageas' portfolio – standalone versus add-on | | | | | | | | |
| • Design a "go-to-market" plan | | | | | | | | |
| • Overcome underwriting challenges and define a pricing concept | | | | | | | | |

**LEGEND:** Kick off | Steering Meetings | Final Presentation | Weekly Meetings

*Table 2: Project's Goals and Timeline*

| IN SCOPE | OUT OF SCOPE |
|---|---|
| Ageas commercial activity in Portugal | Ageas international commercial activities |
| SMEs (all sectors) Households | Micro & large enterprises Freelancers |
| Cyber risk industry (in-depth cyber insurers) | In-depth analysis of IT/cybersecurity providers |
| Cyber insurance | Other insurance products |
| Solutions to overcome underwriting challenges | Underwriting process (operational model) |
| Pricing concept | Stochastic (actuarial) models |
| Key "go-to-market" recommendations | Detailed marketing plan |

***Sources**: Team based*

# The project approach and execution consisted of four phases: diagnosis, analysis, hypothesis testing and the formulation of recommendations.

## B.2.2. Methodology | Project Methodology – Approach

| | Diagnosis | Analysis | Strategy Formulation | Recommendations |
|---|---|---|---|---|
| **Deliverables** | **Kick-off Document** | **Issue Analysis** | **Fact Pack** | **Value Proposition & Action Plan** |
| **Project Actions** | **Theoretical review on Cyber Risk:**<br>• Cyber Risk Definition;<br>• Cyber Risk Value Chain Analysis;<br><br>**Overview of the Cyber Insurance Market:**<br>• Industry Dynamics;<br>• Trends;<br>• Competitive Landscape;<br><br>**Alignment of Expectations:**<br>• Understanding the clients' needs;<br>• Agreeing on the project scope, goals and deliverables;<br>• Settle the project timeframe. | **Issue Analysis:**<br>• Deductive Reasoning;<br>• Inductive Reasoning;<br><br>**External Analysis:**<br>• Industry Analysis (PESTL Analysis);<br>• Industry Profitability Analysis (Market Size, Claim Ratios Porter's Five Force and Product Life Cycle);<br>• Competition Analysis (Benchmark Analysis);<br><br>**Internal Analysis:**<br>• Company Overview;<br>• Ageas Competitive Advantage (Resource-Based View);<br>• Value Chain Analysis (Porter's Value Chain Model);<br>• SWOT & TOWS Analysis. | **Fact Pack Elaboration:**<br>• Hypotheses Formulation and Testing:<br>  • Expert Interviews;<br>  • In-Depth Interviews;<br>  • Surveys. | **Cyber Risk Value Proposition:**<br>• Formulation of different recommendations:<br>  • Target selected clusters;<br>  • Develop a cyber insurance product (coverage and type & structure);<br>  • Go-to-Market Plan;<br>  • Overcoming underwriting challenges & Pricing concept.<br>• Strategic assessment of recommendations;<br><br>**Action Plan:**<br>• Implementation strategy with allocation to different departments and expected timeframe. |
| **Duration** | 1.5 weeks | 7 weeks | 2 weeks | 4.5 weeks |

*Table 3: Methodology used for Project Approach and Execution*

***Sources**: Team based*

# The SCQA framework starts by answering the project's overriding question – followed by its breakdown into MECE arguments and supporting facts – compiled in an issue tree.

## B.2.3. Methodology | Project Methodology – SCQA and Issue Tree Overview

| | |
|---|---|
| **Situation** | Ageas is an international insurance group, with a strong presence in Asia and Europe. The Portuguese branch office is considering expanding its offer to cyber risk insurance, by developing a value proposition for individuals and SMEs. |
| **Complication** | Affirmative cyber risks are not stationary, challenging the usefulness of traditional risk assessment models and the underwriting process. The shortage of technical expertise constrains the capacity to manage this new offer. Moreover, the lack of awareness amongst Portuguese SMEs and individuals results in a low current market value. |
| **Question** | Should Ageas Portugal enter the cyber risk insurance market? |
| **Answer** | **Yes.** |

### Why?

- **External**
  - **Opportunities**
    - Increase in data protection laws and regulations
    - Technological advances improve cybercrime efficiency
    - The future market is expected to be highly profitable
  - **Threats**
    - Mismatch between clients' needs and insurers' offers
    - Rising rivalry due to high profitability and growth potential
- **Internal**
  - **Strengths**
    - Robust financial situation
    - Intangible R&Cs
  - **Weaknesses**
    - High level of OPEX investment
    - Scarcity of data inside the company

### How?

- **Target Customer Segments**
  - Individuals & Families
  - SMEs
  - Selected clusters
- **Offer tailored solutions**
  - **Coverage**
    - PoP: Match competition
    - PoD: Employee Training (B2B)
    - PoD: Comprehensive online protection (B2C)
  - **Type & Structure**
    - Plan-based & Modular framework
    - Standalone (B2B & B2C)
    - Add-on to Home Insurance (B2C)
- **Develop a "Go-to-Market" Plan**
  - Ageas' Brands
  - Distribution channels
  - Awareness & Engagement Strategies
  - Salesforce empowerment
- **Identify Underwriting Solutions**
  - Solutions to manage evolving cyber risks
- **Design a Pricing Concept**
  - Roadmap for adequate pricing

*Figure 2: SCQA Framework & Issue Analysis*

***Sources**: Team based*

# The deductive reasoning is applied through an external and internal analysis to validate the overruling message. Inductive reasoning is developed by formulating hypotheses on how to address the project's challenge.

## B.2.4. Methodology | Project Methodology – Issue Tree

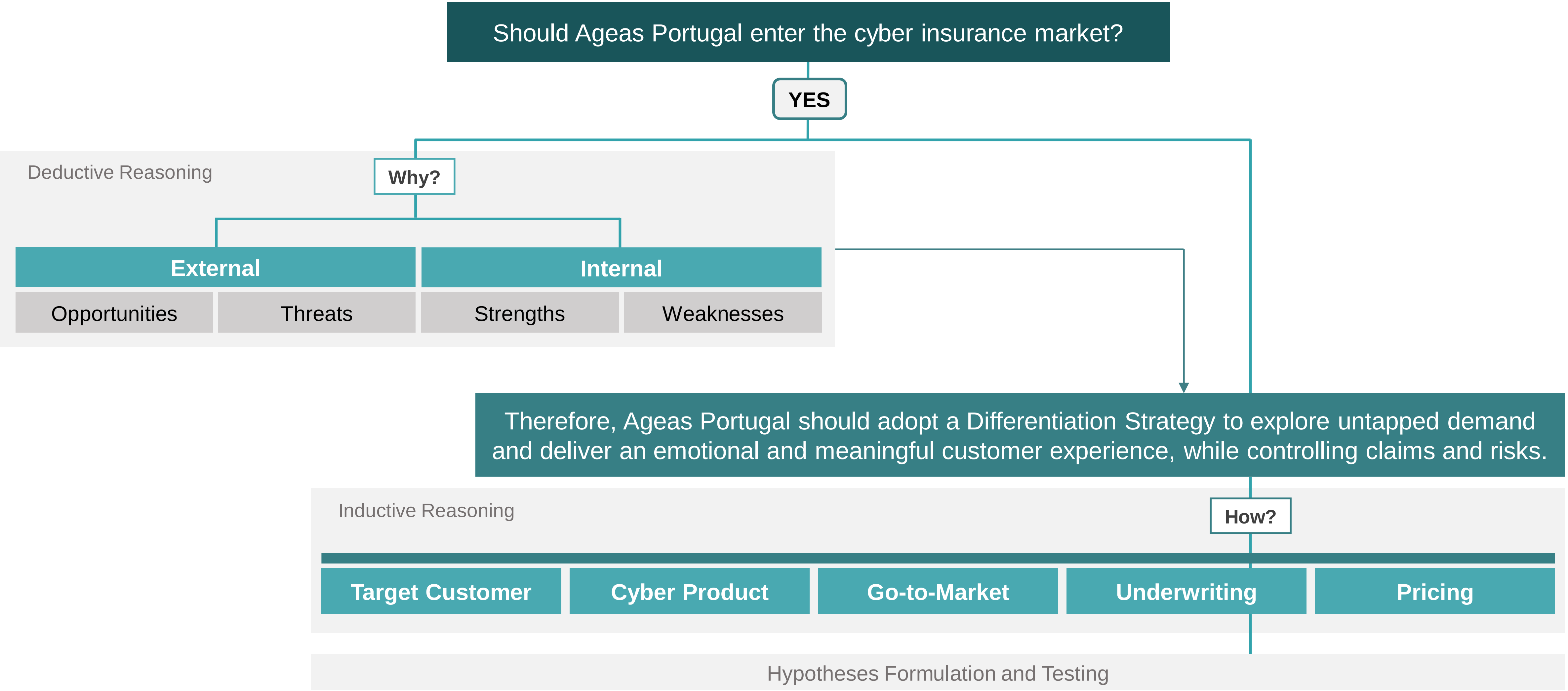



*Figure 3: Issue Tree – deductive and inductive reasoning*

# To understand why Ageas should enter the cyber insurance market, external and internal environments were assessed, looking at opportunities, and threats and identifying the strengths and weaknesses of the company.

## B.2.5. Methodology | Project Methodology – Deductive Reasoning

**Should Ageas Portugal enter the cyber insurance market?**

**YES**

**Why?**

| External | |
|---|---|
| **Opportunities** | **Threats** |
| **Cybersecurity and Data Protection Laws**<br>Have an ambiguous effect on cyber risk. Regulations catalyse improvements on cyber risk awareness, while also increasing losses (with fines and sanctions);<br>**Technological Advances**<br>Improve the efficiency of cyber crime. The shift towards remote work increases cyber vulnerabilities while automatization allows increasingly sophisticated and targeted attacks and expands opportunities along the entire supply chain;<br>**Potential Market**<br>It is expected to be highly profitable – forecast shows high potential market value and low claims ratios. | **Rising Rivalry**<br>The cyber insurance market is facing rising rivalry with the influx of new entrants, due to high profitability and significant growth potential, as well as possible disruptive alternative coverage solutions (e.g. InsurTechs).<br>**Mismatch Between Clients' Needs and Insurers' Offers**<br>There is low market penetration due to a mismatch between clients' needs (tailored and comprehensive policies) and insurers' offers (overly standardized and limited), fostered by the short supply of skilled workers and underwriting and pricing challenges. |

*Table 4: External factors influencing cyber insurance market*

| Internal | |
|---|---|
| **Strengths** | **Weaknesses** |
| **Robust Financial Situation**<br>Provides the required flexibility to follow high risk and high commitment investments.<br>**Intangible R&Cs**<br>A solid client base, extensive ecosystem, strong due diligence negotiation capabilities and technology and innovation-driven culture will facilitate the development of a cyber risk value proposition. | **High-level OPEX investment**<br>Required to develop a cyber risk value proposition, considering the level of risk in achieving market penetration.<br>**Limited specialization, knowledge and experience**<br>Namely lack of historical data and the absence of technical expertise in cybersecurity related departments which constraints the capacity to manage the new offering. |

*Table 5: Internal factors influencing cyber insurance market*

***Sources**: Team based*

# To understand how Ageas should enter this market, recommendations were formulated, focusing on five pillars: target customers, cyber product, go-to-market strategy, underwriting process and pricing concept.

## B.2.6. Methodology | Project Methodology – Inductive Reasoning

**Therefore, Ageas Portugal should adopt a Differentiation Strategy to explore untapped demand and deliver an emotional a meaningful customer experience, while controlling claims and risks.**

**How?**

| Target Customers | Cyber Product | Go-to-Market | Underwriting | Pricing |
|---|---|---|---|---|
| Target customer segments | Offer tailored solutions | Develop a "Go-to-Market" Plan | Identify underwriting solutions | Design a pricing concept |
| Clustering customer segments based on the most relevant characterization variables to determine needs and preferences, enabling tailored solutions. | Differentiate and adopt an universal language; offer comprehensive and flexible coverage to allow clients to build tailored policies (multiple plans to be complemented with optional modules). | Design a customer journey map; rank Ageas' brands to place CyberShield; select distribution channels; develop awareness and engagement strategies and empower salesforce. | Identify strategic options and solutions to surpass underwriting challenges and control risks of tailored and comprehensive cyber solutions. | Incorporate customer, cost and competition orientation to achieve adequate pricing. |

**Note:** Recommendations designed after hypotheses analysis and validation (see next slide).

*Figure 4: Inductive Reasoning*

***Sources**: Team based*

# Hypotheses formulation was followed by respective validation, through a rigorous analysis using secondary data, benchmarking, in-depth interviews and surveys.

## B.2.7. Methodology | Project Methodology – Hypotheses Analysis

**Note:** Only validated hypotheses are presented in the table below.

| ISSUE | SUBISSUE | HYPOTHESIS | ANALYSIS |
|---|---|---|---|
| **Target** | Should Ageas target selected clusters? | Yes. By grouping customers according to characterization variables, Ageas assures it keeps a maximum level of risk (by not targeting highly exposed and unprotected companies) and it can offer a product tailored to the clusters' needs. | • Secondary Data<br>• Surveys |
| **Cyber Product** | Should Ageas match the competition in the coverage offered? | Yes. Ageas should match the competition's offer, since the lack of points of parity may be a reason not to choose the product. | • Secondary Data (potential partnerships & SMEs' and Individuals' needs and preferences)<br>• Benchmarking & BPs analysis<br>• In-depth Interviews<br>• Surveys |
| | Should Ageas exceed the competition in the coverage offered? | Yes. Offering a differentiating product that creates value to the customers will increase market penetration. | |
| | Should Ageas develop a plan-based and modular framework for its offer? | Yes. Flexibility is highly valued while standardized and limited coverages are two of the reasons behind low market penetration. | |
| | Should Ageas develop the offer as a standalone product? | Yes. The complexity of the product for the B2B segment requires a standalone policy. Moreover, it prevents silent cyber risks[1]. | |
| | Should Ageas develop the offer as an add-on to a multi-risk policy? | Yes. Since the product is not as complex for the B2C segment, it can be developed either as a standalone or as an add-on to a multi-risk policy. | |
| **Go-to-Market Plan** | Can Ageas develop an efficient Go-to-Market Plan? | Yes. By considering the customer journey, Ageas will be able to evaluate its brands, select appropriate distribution channels, develop awareness tools, empower sales' force and ultimately achieve an efficient Go-to-Market Plan. | • Secondary Data<br>• Benchmarking & BPs analysis<br>• Surveys |
| **Underwriting** | Can Ageas overcome underwriting challenges? | Yes. By correctly identifying underwriting challenges and the appropriate strategic options and solutions to surpass them. | • Secondary Data<br>• Benchmarking & BPs analysis |
| **Pricing** | Can Ageas implement an efficient pricing concept? | Yes. By taking into account all the variables that influence price (cost, competition and costumer) as well as the flexibility of the offer, Ageas will be able to implement an efficient pricing concept. | |

*Table 6: Hypothesis Analysis*

[1]Further developed in Underwriting (recommendation 6). ***Sources**: Team Based*

# Academic frameworks were used and adapted to assess the internal and external situation of the company, as well as to formulate recommendations, grounded on qualitative and quantitative research methods.

## B.2.8. Methodology | Project Methodology – Investigation Methods

### Deductive Reasoning – WHY?

| External Analysis | | Internal Analysis |
|---|---|---|
| PESTL | Macro Context | Resource-Based View |
| Porter's Five Forces | Micro Context | Porter's Value Chain Model |
| Competition Analysis | | |
| Industry Life Cycle | | SWOT &TOWS Analysis |
| Profitability Indicators (Market Size & Claims Ratio) | | |

*Figure 5: Investigation Methods - Deductive Reasoning*

### Inductive Reasoning – HOW?

- Porter's Generic Competitive Strategies
- STP Model (Segmentation, Positioning and Targeting)
- Marketing Mix (Adapted) – 7Ps
  - Cyber Coverage, Type & Structure (Product)
  - "Go-to-Market" Plan (Place, Promotion, People, Physical Evidence)
  - Underwriting Solutions (Processes)
  - Pricing Concept (Price)

*Figure 6: Investigation Methods - Inductive Reasoning*

| Sources | | | | | |
|---|---|---|---|---|---|
| **Internal Company Data** | **Industry Experts Interviews**<br>11 Experts | **Secondary Data Academic Papers Review** | **Benchmark Analysis**<br>Direct and Indirect Competition | **Customers' In-Depth Interviews**<br>B2B: 4 interviews<br>B2C: 10 interviews | **Surveys**<br>B2B: 47 answers<br>B2C: 525 Answers |

*Table 7: Project Sources*

***Sources**: Team based*

# Ageas is a multinational insurance group with a presence in Portugal since 2005. Since then, the group has done strategic acquisitions and ventures that contributed to establishing itself as one of the biggest players in the country.

## C.1. Diagnosis | Company Overview (I/II)

### Company's ID:

| | |
|---|---|
| 1824 | Fortis Holdings was founded |
| 2010 | Renamed as Ageas |
| 15 | Countries[1] |
| 26 | Partners |

*Figure 7: Ageas Group International Presence*

*In Portugal:*

| | |
|---|---|
| 1.304 | Employees |
| 1.797K | Clients |
| 3.382 | Agents & Brokers |
| 2 | Segments: B2B & B2C |

### Timeline

**2005** – Ageas **enters** in **Portugal** through **Médis** and **Ocidental** (in partnership with Millennium BCP).

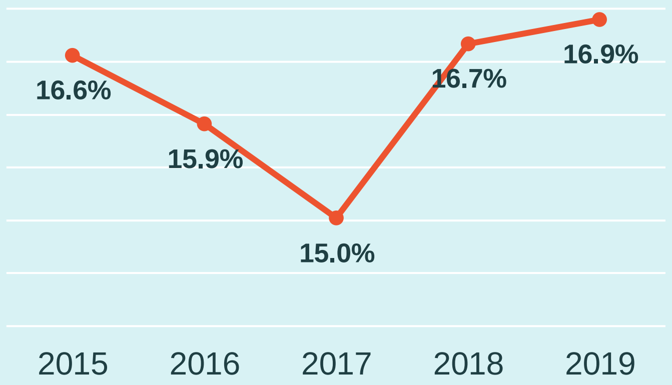
**2016** – **Acquisition** of **AXA Portugal** and **Direct** (currently Ageas Seguros and Seguro Directo). Portugal becomes the 2nd **home market**.

**2017** – Ageas Portugal is 2nd **player** in **life**, 3rd in **non-life** and 2nd in **overall ranking**.

**2019** – **Joint venture** with National Association of **Pharmacies** – Go Far and **launch** of **Clínica Médis** dental cliniques.

*Figure 8: Ageas Portugal History*

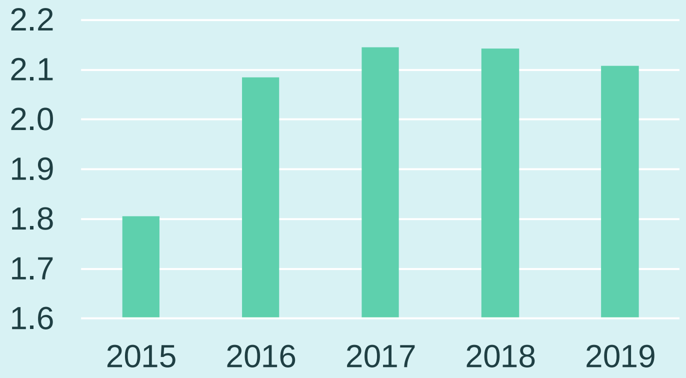
### MARKET SHARE IN THE LAST 5 YEARS




*Graph 1: Ageas Portugal market share in the last 5 years*

### PREMIUMS IN THE LAST 5 YEARS

[Values in €B]




*Graph 2: Ageas Portugal premiums in the last 5 years*

[1]Belgium, UK, Portugal, France, Turkey, China, Malaysia, Thailand, India, the Philippines, Vietnam, Laos, Cambodia and Singapore.

***Sources**: Ageas Group, Ageas Portugal, ECO*

# Ageas group mission, vision and strategy are aligned with the company's diverse portfolio of insurance and beyond insurance brands, with presence in multiple business lines.

## C.1. Diagnosis | Company Overview (II/II)

### Company's Strategy

| | |
|---|---|
| **MISSION** | "To deliver an emotional and meaningful experience into people's lives." |
| **VISION** | "Become the reference partner in insurance, a relevant player in services and the best place to work for entrepreneurs." |
| **STRATEGY** | "*Our story begins with the customer. We exist for our customers*." Connect 21 is the Strategy of Ageas PT for the next 3 years, focused on the following strategic choices: *"(1) focus on great customer experience; (2) by preventing, preparing, protecting, assisting and beyond; (3) through partnerships and innovation driven by technology; (4) as one agile organisation; (5) to achieve sustainable growth and to create social impact."* |

*Table 8: Ageas' Strategy and Values*

Focusing on six lines of business:

Life | Accident & Assistance | Property & Commercial | Motor | Liability | Financial

Non-Life

Company's portfolio:

Insurance:

- **Ageas Seguros:** Life, Non-Life and Health;
- **Médis:** Health;
- **Seguro Directo:** Direct company specialized in Motor insurance;
- **Ageas Pensões:** Pension Fund Manager;
- **Ocidental:** Bancassurance (Life & Non-Life).

Beyond insurance:

ageas repara, clinicamédis, Go Far, KLEYA, MUNDO ageas

### CYBER RISK INSURANCE OBTAINABLE MARKET SIZE

| | Current: 2020 | Potential: 2025 |
|---|---|---|
| **B2B** | **€ 2.1M** | **€ 5.4M** |
| **B2C** | **€ 2.6M** | **€ 5.7M** |

*Table 9: Cyber Risk Obtainable Market Size*

**Note:** See slide 23 for the reasoning applied.

***Sources**: Ageas Portugal*

# To develop a successful value proposition, it was crucial to define and characterize cyber risk and cybersecurity. NIST Framework was used as the best practice for cybersecurity risk management.

## C.2. Diagnosis | Cyber Risk and Cybersecurity Definition

| Cyber Risk and Cybersecurity Definitions | The **risk**[1] - *"effect of uncertainty on objectives"* – of **cybersecurity**[2] – *"a set of preventive, monitoring, detection, reaction, analysis and correction measures and actions aimed at maintaining the desired security level and guaranteeing the confidentiality, integrity, availability and non-repudiation of the information, networks and information systems in the cyberspace, and the people that interact in it".* |
|---|---|

### Likelihood × Consequences

**Likelihood**

Potential of a threat exploiting a vulnerability

**Threats**

**Agent**
- **Internal** (Direct)
- **External** (Indirect)

**Source:**
- **Criminal**
  - Corporate espionage
  - Terrorism
  - Hacktivism
  - Geopolitical
- **Non-criminal**:
  - Unintentional human behavior

**Vulnerabilities**

- **Technology-based:** weaknesses of computer assets (software/ hardware level)
- **Human-based:** lack of security awareness training

There has been a shift from technology-based to social engineering attacks.

**Consequences**

**Direct** (Measurable)
- Business interruption
- Asset loss/replacement
- Legal & judicial

**Indirect** (Non-measurable):
- Reputational
- Psychological/ emotional
- Physical
- Brand value
- Stock price impact
- Difficulty in attracting and retaining talent

*Figure 9: Dimensions to characterize and evaluate the magnitude of cyber risk*

| Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|
| Asset Management<br>Business environment<br>Governance<br>Risk Assessment | Awareness and Training<br>Data Security<br>Information Protection, Processes & Procedures<br>Maintenance | Anomalies & Events<br>Security & Continuous Monitoring<br>Detection Processes | Response Planning<br>Communication<br>Analysis<br>Mitigation<br>Improvements | Recovery Planning<br>Improvements<br>Communication |

*Figure 10: NIST Framework (standards, guidelines and best practices to manage cybersecurity risk)*

| Confidentiality | Integrity | Availability | Nonrepudiation |
|---|---|---|---|
| *"Not made available or disclosed to unauthorized individuals, entities, or processes"* | *"Accuracy and completeness"* | *"Accessible and usable on demand by an authorized entity"* | *"Ability to prove the occurrence of a claimed event or action and its originating entities"* |

*Figure 11: Four Cybersecurity Pillars[1]*

[1] ISO/IEC 27000 [2] ENSC ***Sources***: *Industry experts interviews, ISO, CNCS, ENCS, ENISA, Team-based*

# Cyber insurance is typically composed of pre-breach services – in partnership with IT and cybersecurity providers - and general coverage – divided into 1st party, 3rd party and other benefits, according to ENISA framework.

## C.3. Diagnosis | Introduction to Cyber Insurance

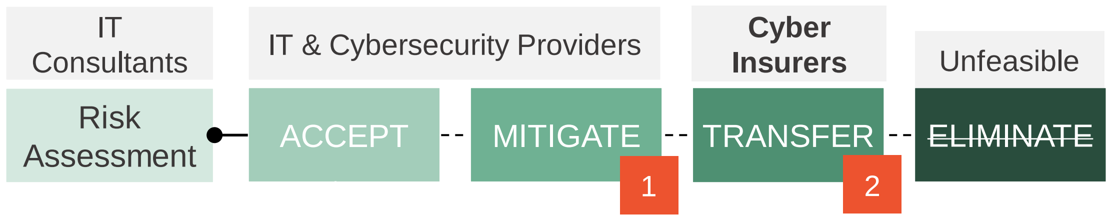



*Figure 12: Responses to Cyber Risk*

Most cyber insurance products already combine risk transfer and risk mitigating (in partnership with IT & Cybersecurity Providers)

| 1 Pre-breach services | | |
|---|---|---|
| **Risk Assessment** | **Risk Mitigation** | **Contingency Norms** |
| Vulnerability Analysis and Resolution | Back-up system and encryption configuration | Safety Manual - Recommendations |
| Web Vulnerabilities Research | Network Security - AV, Firewalls, Wi-Fi and output connections and control recovery of pirated accounts. | GDPR Compliance Evaluation and Guide |
| | Anti-Hijacking App | |

*Table 10: Pre-breach services*

| | 2 General Cyber Insurance Coverage Types | | |
|---|---|---|---|
| | 1st Party | 3rd Party | Other Benefits |
| **Definition (ENISA)** | Coverage against direct losses incurred by the insured, mostly consisting of business interruption and costs associated with mitigating a cybersecurity event. | Liability coverage indemnifying companies for losses to others. | Related to assorted costs and services. |
| **Features** | Business Interruption | Data Protection and Cyber Liability | Forensic Investigation Costs |
| | Cyber Extortion | Media Liability | Legal Advice and Defense |
| | Data & Software Reconstitution | Wrongful collection of information | Notification Costs |
| | Regulatory Fines and Sanctions | Media content infringement/ defamatory content | Credit / Identity Monitoring |
| | | Violation of notification obligations | Communication Costs |

*Table 11: General Cyber Insurance Coverage*

***Sources**: Industry experts interviews, ENISA, Team-based*

# Covid 19 Pandemics has impacted negatively socioeconomic environment. Nevertheless, the rise in cybercrime, allied to technological innovation may favour the cyber insurance industry.

## D.1.1. Analysis | External Analysis | PESTL

Further Detail: Appendix 2

### Political

- **Covid-19 Pandemics** imposing political changes worldwide;
- **Brexit** allowing for growing anti-EU parties which threatens the union's stability;
- Recent outcome in the **US elections** may ease tensions in trade;
- Public investment on cybersecurity – with the creation of *Centro Nacional de Cibersegurança.*

### Economic

**Covid-19 Pandemics** economic impact**:**

- **Economic Recovery:** GDP expected to decline 9.5% in 2020, recovering 5.2% in 2021;
- **Unemployment** will peak in 2021 and remain above pre-crisis level until 2022;
- **Private consumption** is expected to start recovering in 2021.

### Social

**Covid-19 pandemics** social impact:

- Change in consumer behavior – the sharp rise in online shopping;
- **Shift to remote work** leading to increasing awareness of cyber risks.

**Portuguese population:**

- Aging population;
- Medium-low-income level;
- Growing literacy levels.

### Technological

- **Cloud-based services & 5G** expanding cyber-attacks' opportunities along the entire supply chain;
- **Artificial Intelligence** automates the cybercriminal process, allowing for increasingly sophisticated and targeted cyber attacks;
- Companies' **digital innovation** is higher than their ability to secure it.

### Legal

**Data protection and cybersecurity laws** increasing awareness of cyber risk:

- **GDPR:** provisions on notifying and indemnifying data breaches;
- **NIS Directive:** particularly towards DSPs and OESs of EU countries;
- **EU Cybersecurity Act:** certification for digital products, services and processes in the EU.

***Sources****: The Balance, Banco de Portugal, INE, Pordata, The Economist, Kaspersky, Entrust Solutions, GDPR.EU, ENISA*

# Even though there is a low threat of substitutes, the high bargaining power of suppliers (given the highly differentiated input) and the high competitive rivalry impact negatively the industry's profitability.

## D.1.2. Analysis | External Analysis | Porter's Five Forces

Further Detail: Appendix 3

### Threat Of New Entrants

- Capital requirements: **High** (particularly in research and advertising)
- Access to channels: **High** (growing online channels with low required investments)
- Legal requirements: **High**

Overall: **MEDIUM**

### Threat Of Substitutes

- Economic substitutes: **Low**
- Beneficial substitutes: **Low**
- Switching costs: **Medium**

Alternatives as savings/ investments and "self-insurance" are inefficient due to the unpredictability of cyber risks.

Overall: **LOW**

### Bargaining Power Of Suppliers

- Differentiated input: **High**
- Backward Integration: **Low**
- Substitute inputs: **Low**
- Size of suppliers: **High**
- Supplier switching costs: **High**

Overall: **HIGH**

### Bargaining Power Of Buyers

- Price sensitivity: **High**
- Buyer size: **Low**
- Product differentiation: **Low**
- Switching costs: **Medium**
- Customer loyalty: **Low**
- Information access: **High**

Overall: **MEDIUM**

### Competition Rivalry

- Product differentiation: **Low**
- Industry concentration: **High**
- Number of competitors: **Medium**
- Industry growth: **High**
- Entry barriers: **Medium**
- Exit barriers: **High**

Overall: **HIGH**

***Sources***: *MarketLine, Team Based*

# To measure current and potential market size, the chain ratio method was used, with the necessary and relevant assumptions. Afterwards, the robustness of the values obtained was confirmed through extrapolation.

Further Detail: Appendix 4

## D.1.3. Analysis | External Analysis | Market Size Methodology (I/II)

### Method 1 – Chain-ratio Method

1 Forecast the **VOLUME**

**Total Available Market**

SMEs and families with the need & financial ability to buy cyber insurance

Willingness to buy or replace

**Serviceable Available Market**

SMEs and families with or willing to buy cyber insurance

Market Share

**Serviceable Obtainable Market**

Ageas reasonably expects to acquire.

*Figure 13: Chain Ratio Method to forecast market size[1]*

Assumptions:

- Industry is a relevant factor to cyber exposure.
- SMEs' exposure indicates the SMEs' urgency to buy.
- Families will not spend more than 0.35% of their income.

- SMEs with high or total willingness to buy or to replace.
- Individuals with high or total willingness to buy.

- Ageas' market share (Non-Life branch) – SMEs.
- Market is equally distributed amongst players – families.

2 Forecast the **PRICE**

WTP from respondents of Serviceable Available Market.

3 Consider Market Evolution

- Volume adjusted to annual growth rate.

Current Market Size: 2020

Potential Market Size: 2025*

- SMEs WTB = % of Spanish SMEs with cyber insurance (2019)
- Families' WTB = % of respondents with paid online protection

### Method 2 - Extrapolation

1 Extrapolation Variables:

- Gross Domestic Product (GDP);
- Global Cybersecurity Index (GCI);
- Cyber Attacks Rate (CAR);

2 Weights were attributed to variables

- According to its impact on cyber products.

3 Extrapolation

- Italy's cyber insurance market value
- Purchasing Power Parity (PPP) adjustment

4 Breakdown – B2B & B2C Segment

- US distribution of market value

**Note:** Detailed explanation of the methodology applied is on appendix 4.

[1]Kerin and Peterson 2010

***Sources***: *Kerin and Peterson 2010, Team based, Experts Interviews, Surveys, PORDATA, INE, Orbis, Eurostat, OECD, McKinsey, Verizon, NAICS, Ageas Portugal, Enterprise Ireland (Global Ambition); ITU; World Development Indicators; Microsoft, KPMG, Swiss RE*

# The values obtained in methods 1 and 2 confirm the robustness of the forecasted market size and indicate great potential for Ageas in this market. These values can be leveraged with the inclusion of beyond insurance.

grupo ageas portugal

Further Detail: Appendix 4

## D.1.3. Analysis | External Analysis | Market Size Results (II/II)

**Method 1**

| Current: 2020 | Potential: 2025* | Current: 2020 | Potential: 2025* |
|---|---|---|---|
| **1.** Average Annual Premium: €1 900 | | **1.** Average Annual Premium: €66 | |
| **2.** Total Available Market (TAM) | | **2.** Total Available Market (TAM) | |
| Most Affected Sectors **25.4K** | + Least Affected Sectors (AGR) **61.1K** | Annual Income >19K **1.56M** | Annual Income >19K (AGR) **2.02M** |
| **3.** Serviceable Available Market (SAM) | | **3.** Serviceable Available Market (SAM) | |
| Willingness to Buy – **30%** | Willingness to Buy – **32%** | Willingness to Buy – **10%** | Willingness to Buy – **17%** |
| **7.6K** → **€15.1M** | **19.5K** → **€ 38.9M** | **156K** → **€10.3M** | **343K** → **€ 22.7M** |
| **4.** Serviceable Obtainable Market (SOM) | | **4.** Serviceable Obtainable Market (SOM) | |
| **1050** → **€2.1M** | **2697** → **€ 5.4M** | **39K** → **€2.6M** | **86K** → **€ 5.7M** |

*Table 12: Market Size Results (Chain Ratio Method)*

**Method 2**

| | Current: 2020 (companies) | | Current: 2020 (households) |
|---|---|---|---|
| **3.** Serviceable Available Market (SAM) | **€17.7M[1]** | **3.** Serviceable Available Market (SAM) | **€11.8M** |
| **4.** Serviceable Obtainable Market (SOM) | **€2.5M[1]** | **4.** Serviceable Obtainable Market (SOM) | **€3M** |

*Table 13: Market Size Results (Extrapolation Method)*

The values of method 2 confirm the robustness of method 1 and consequently, of the forecasted market size.

### Key Takeaways

1. Cyber insurance market holds great potential: serviceable and obtainable market sizes are predicted to duplicate in 5 years.
2. The inclusion of beyond insurance may enlarge the market size forecast.
3. Insurers that enter the cyber risk market now will obtain the know-how crucial to gain a first-mover advantage and reap the long-term benefits.

[1] Also includes large and micro companies; ***Sources****: Team based, Experts Interviews, Surveys, PORDATA, INE, Orbis, Eurostat, OECD, McKinsey, Verizon, NAICS, Ageas Portugal, Enterprise Ireland (Global Ambition); ITU; World Development Indicators; Microsoft, KPMG, Swiss RE*

# The loss and combined ratios in Portugal – extrapolated from the US market and adjusted to the cybersecurity index – confirm the industry's profitability.

## D.1.3. Analysis | External Analysis | Claims Ratios

Further Detail: Appendix 5

### Extrapolation Variable

The **Global Cybersecurity Index** (GCI) measures the commitment of countries to cybersecurity, along **five pillars:** i) Legal Measures; ii) Technical Measures; iii) Organizational Measures; iv) Capacity Building; v) Cooperation

| | Global Cybersecurity Index (2018) |
|---|---|
| US | 0.926 |
| Portugal | 0.758 |

*Table 14: Cybersecurity Index*

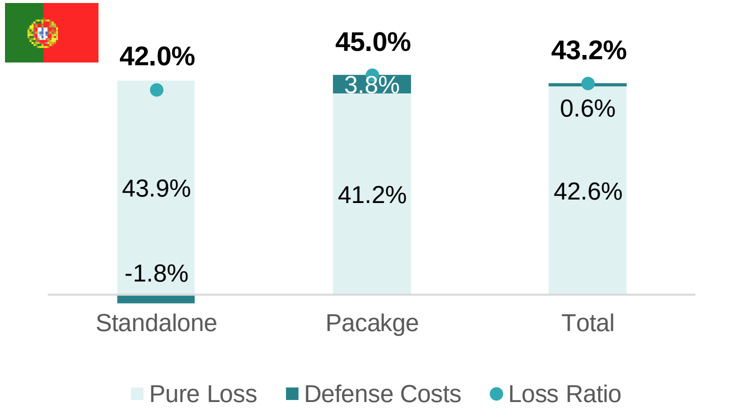
### Reasoning For Extrapolation

The higher the GCI, the lower the number of cyber attacks (on average), implying lower claims ratios (both loss and combined ratios) – **negative relationship**. As GCI is lower in Portugal than in the US, loss and combined ratios are expected to be higher.

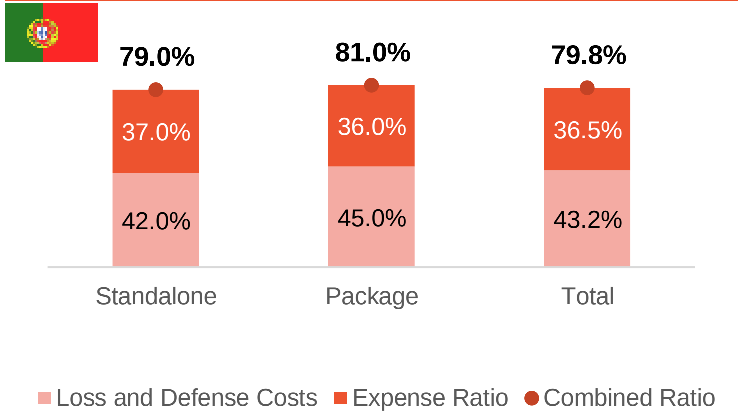
### Loss and Combined Ratios

The **loss ratio** measures the total incurred losses in terms of the total collected insurance premiums, while the **combined ratio** measures the incurred losses and expenses concerning total collected premiums. Given that both ratios are **below 100%,** the cyber insurance industry is considered to be relatively **profitable.**

**Loss Ratio**




**Combined Ratio**




*Graphs 3 and 4: Loss and Combined Ratios in Portugal*

***Extrapolated** from **US overall market, 2018**

***Sources**: AON, ITU*

# The cyber insurance product is currently in the growth stage of the product life cycle, characterized by a steady increase in sales and profits, and requiring product differentiation and effective marketing.

## D.1.4. Analysis | External Analysis | Product Life Cycle

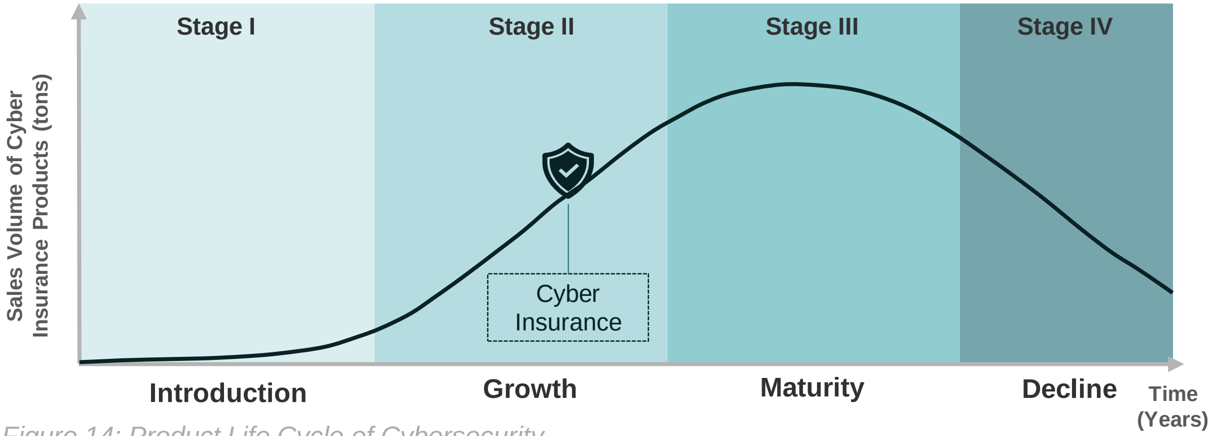


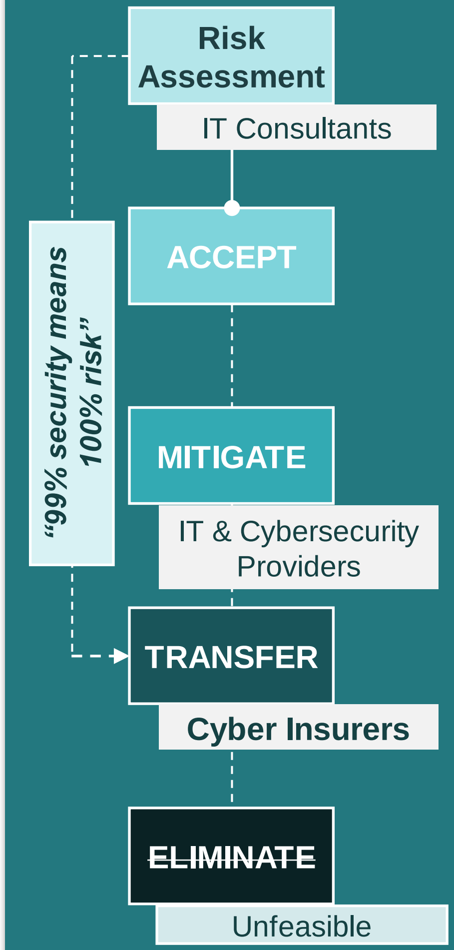

*Figure 14: Product Life Cycle of Cybersecurity*

| | Stage II - Growth |
|---|---|
| **Sales** | • Rapidly rising |
| **Costs** | • Lower average cost |
| **Buyers** | • Early adopters |
| **Profits** | • Rising profits |
| **Competitors** | • Growing number |
| **Products** | • Quality differentiation |
| **Marketing** | • High advertising |
| **Strategy** | • Good marketing |

*Table 15: Characterization of Stage II (Growth) of Product Life Cycle*

The second stage of the product life cycle is characterized by a rapid increase in sales and rising profits and it requires quality differentiation as well as good marketing.

### Cyber Insurance (Stage II)




The **increase in cyber threats**, due to the **expansion of the online ecosystem**, enabled the appearance of **several responses to cyber threats**. While **IT Consultants** focus is on **risk assessment**, **IT & Cybersecurity Providers** put their efforts into **risk mitigation**. **Insurers** saw an opportunity in **cyber risk transfer**, since it was impossible to guarantee 100% security and entered the market in the late 1990s.

In recent years, the market size has been continuously growing at a CAGR of around 20-25%, with sales volume reaching values of $3-4bn globally[1].

*Figure 15: Responses to Cyber Risk*

[1] 2017 values; ***Sources***: *Team based, KPMG*

# In the B2B segment, there is a considerable number of direct and indirect competitors acting in the different lines of cybersecurity. In the B2C segment, direct and indirect competition is smaller but expected to rise in the future.

## D.1.5. Analysis | External Analysis | Competition Analysis (I/II)

International benchmark and BPs on Appendix 6

### Indirect Competition

**B2B**

**IT Consultants**

accenture, Capgemini, Deloitte.

**IT Providers**

Microsoft, ORACLE, IBM, CISCO

**Cybersecurity Providers**

Identity & Access Management: okta, PingIdentity, FORGEROCK

Training & Education: INTEGRITY, DefenceBit

Software Level: SecurityScorecard, FORTINET, claranet, MANDIANT, Check Point, FIREEYE, S21sec, BITSIGHT, DARKTRACE, Symantec, McAfee

**Note:** Most of the companies represented offer various cybersecurity solutions worldwide.

### Direct Competition

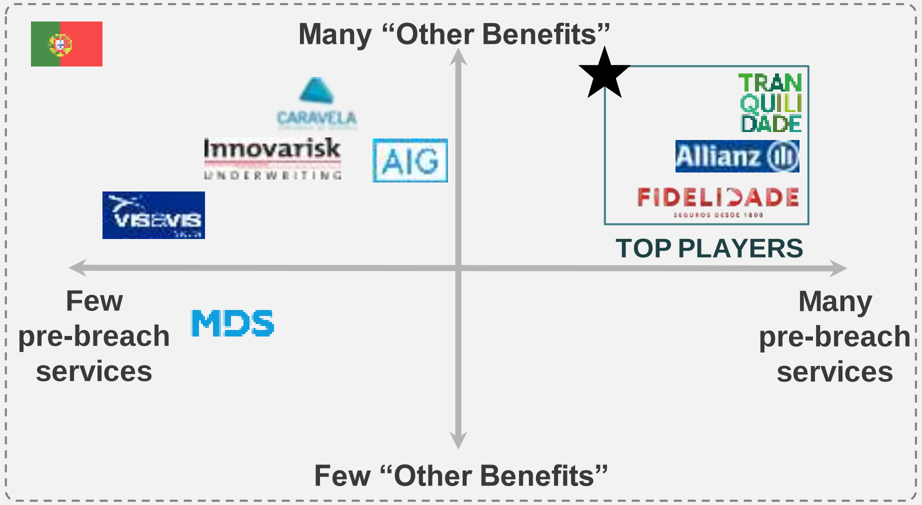



*Figure 16: Perceptual Map*

Other players: MARSH, CHUBB, SEPTOR, AJSEG, Seguros 24

**B2C**

**Online Protection Providers**

TOTAL AV, panda, intego, eset

**Parental Control Providers**

Net Nanny, Qustodio

Online protection brands that also offer packages with parental control features:

McAfee Total Protection, Kaspersky, Norton 360, Bitdefender Family Pack

Only two insurers offer personal cyber insurance.

| TARGET: FAMILIES | FIDELIDADE | Inter Partner ASSISTANCE |
|---|---|---|
| PRICE (year) | Plan 1: €36 \| Plan 2: €48 | €60 |

*Figure 17: Personal Cyber Insurance Offer*

*Sources: Team based, FoundationCapital 2019, AIG, AJSEG, Allianz, Caravela, Chubb, Fidelidade, Innovarisk, Marsh, MDS, Septor, Tranquilidade, Visavis, Seguros 24, Inter Partner Asssistance*

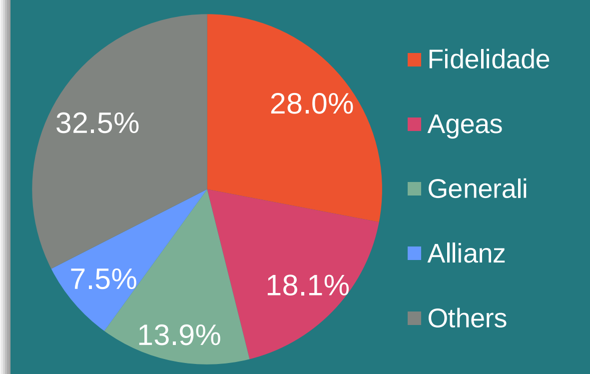
# The three top players in the B2B segment offer a standalone product, with pre and post-breach services. In the B2C segment, the only two players offer a standalone product, with few pre-breach services.

## D.1.5. Analysis | External Analysis | Competition Analysis (II/II)

| | | B2B Segment | | B2C Segment | |
|---|---|---|---|---|---|
| | | FIDELIDADE | TRANQUILIDADE | Allianz | FIDELIDADE | Inter Partner Assistance |
| TYPE AND STRUCTURE | | - Standalone<br>- Base with one add-on | - Standalone<br>- Base with two add-ons | - Standalone<br>- Four plans | - Standalone<br>- 2 Plans | - Standalone<br>- Standardized |
| PRE-BREACH SERVICES | | **(1)** Vulnerability analysis & resolution; **(2)** Web research analysis; **(3)** GPPR compliance evaluation and guide; **(4)** Safety manual; **(5)** Back-up system encryption configuration; **(6)** Control recovery of pirated accounts; **(7)** Updates devices, verification and configuration of AV, firewalls, Wi-Fi, output connections; **(8)** Anti-hijacking app | | | Back-up System configuration | Identity & Access Management |
| POST-BREACH SERVICES | 1ST PARTY | **(1)** Loss of incomes & extra expenses; **(2)** data/software reconstitution and **(3)** regulatory fines & sanctions | | | **LEGAL COVERAGE:**<br>- Fraudulent use of payment methods;<br>- Civil Responsibility;<br>- Complaint of online shopping contracts.<br>**ASSISTANCE COVERAGE:**<br>- Tracking and deleting sensitive information;<br>- Devices geolocation & block;<br>- Technical assistance;<br>- Psychological Counselling. | **WARRANTIES:**<br>- Fraudulent use of payment methods;<br>- Online Shopping;<br>- Online Reputation Management;<br>- Identity theft. |
| | | **(4)** Extortion | **(4)** Extortion<br>**(5)** IP theft | | | |
| | 3RD PARTY | *"Payment of Indemnities that the Insured is legally obliged to pay, for damages and losses caused to 3rd parties/employees."* | | | | |
| | OTHER BENEFITS | **(1)** Forensic Investigation; **(2)** Legal Advice and Defence; **(3)** Credit/ID Monitoring; **(4)** Notifications and **(5)** Communications (Public Relations) | | | | |

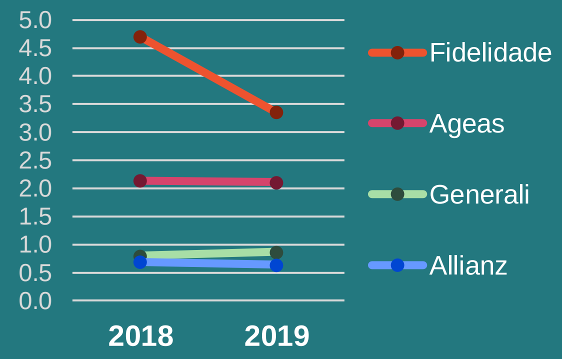
*Table 16: Portuguese benchmark analysis of 3 main players of cyber insurance for companies*

### MARKET SHARE
[1st semester 2020 Values]




*Graph 5: Market Shares (1st semester – 2020)*

### PREMIUMS
[Values in €B]




*Graph 6: Premiums (2018, 2019)*

# To understand the contribution of the different activities of Ageas to value creation, an adaptation of Porter's Value Chain Model specific to the insurance industry was used.

## D.2.1. Analysis | Internal Analysis | Porter's Value Chain Model (I/II)

### Adaptation of the Porter's Value Chain Model to the Insurance Industry

**Porter's Value Chain Model:** Disaggregation of the company's (and its product's or service offerings') activities into strategically relevant steps that contribute to value creation. Since Porter's Model was created for general industries, the team used an insurance-specific adaptation from KPMG Germany (2020) for the analysis of Ageas' value chain.

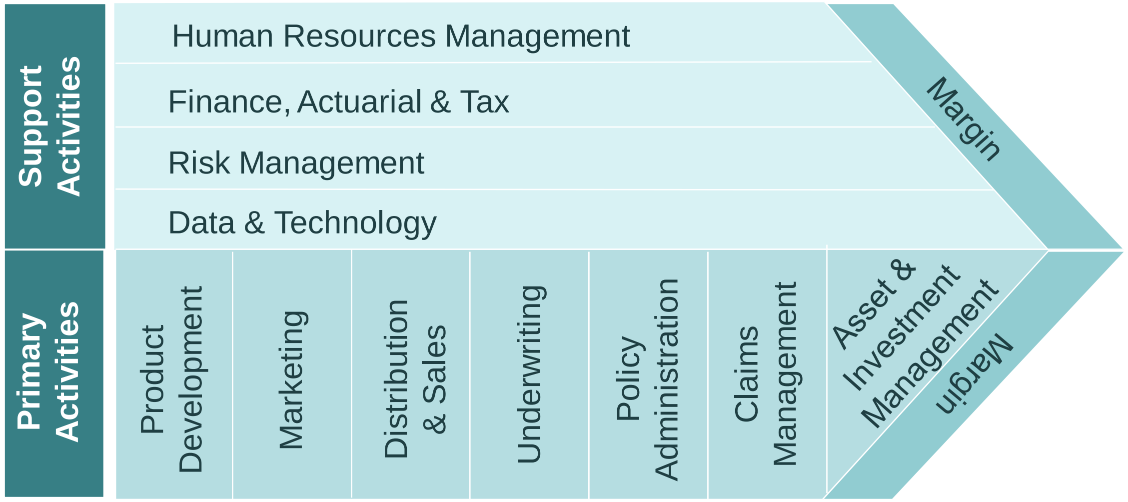



*Figure 18: Insurance adaptation of Porter's Value Chain Model*

### Support Activities

- **Human Resources Management:** concerns **human capital management**. Ageas **creates value** through the **effective engagement** of **people**, with different initiatives promoting **organizational pride** and impacting the community, such as corporate social responsibility and sustainability.
- **Finance, Actuarial & Tax:** includes the **management** and **report** of **finances**, **tax** and **actuarial**. Through the use of **technology innovation**, namely InsurTech, process automation and artificial intelligence, Ageas can **develop cost efficiencies** and, thus, **create value**.
- **Risk Management:** strategies to implement **risk assessment**, **mitigation** and **monitoring measures**. Ageas already includes these measures in its business lines, **reducing its exposure** and **preventing higher losses**.
- **Data & Technology:** involves the **management** and **monitorization** of **IT infrastructure** (hardware & software). Ageas **creates value** by embracing **technology disruption**, through partnerships (e.g. SAP Ariba platform).

***Sources**: Porter's Value Chain Model, KPMG, Ageas Portugal*

# The main challenges identified in the cyber insurance value creation are related to the development of a tailored product, the respective marketing and distribution and the underwriting process.

## D.2.1. Analysis | Internal Analysis | Porter's Value Chain Model (II/II)

### Primary Activities

- **Product (and Service) Development:** **design**, **development** and **launch** of **new products** and **services**. Ageas' Business Development team **creates value** with the gathering of **market** and **consumer data** and **insights** translated into a product that **meets clients' needs** and **preferences**.
- **Marketing:** **brand management**, **advertising** and **customer engagement**. The Marketing department **creates value** with **brand** and **trust messages**, connecting with the client (Ageas Seguros won the bronze trophy at the Gala of Communication Effectiveness Awards).
- **Distribution and Sales:** tackles **strategic market penetration**. Ageas' agents and brokers **create value** by **effectively delivering** the product's **message** on the preferred channels and **advising** current and potential clients.
- **Underwriting:** **assessment** of **profiles** and **pricing** to **issue policies**. Ageas **leverages** on its **data-driven operational model** as well as on **cancellation**, **renewal** and **retention expectations** to assess potential **exposures** and **opportunities.**
- **Policy Administration:** **managing** the entire **policy life cycle**. Ageas **capitalizes** on **processes' automation** to **create value** through **cost efficiencies**.
- **Claims Management:** claims **assessment** and **agreement**. A **technology-enabled** process at Ageas, with the settling of **maximum claim value** and **non-payment** of claims **review** **decreases** company's **exposure** and **prevents** higher **losses**.
- **Asset and Investment Management:** management of **assets**, from **policyholder** to **surplus**. One of the main **revenue-generators** at Ageas, besides premiums and beyond insurance activities, is the **leveraging** and **investment** on **assets**.

### Key Takeaways

Main challenges on Cyber Insurance value creation:

1. Developing a product tailored to customers' needs
2. Marketing, Distribution & Sales (Go-to-Market)
3. Underwriting

The team will present solutions to these challenges on the value proposition.

*Sources*: *Porter's Value Chain Model, KPMG, Ageas Portugal*

# The resource-based view model was used to identify the firm's resources that fulfil the VRIO criteria and, thereby, have the potential to deliver a sustainable competitive advantage to the company.

## D.2.2. Analysis | Internal Analysis | Resource-based View (I/II)

### VRIO CRITERIA

**VALUE:** enables a firm to exploit an opportunity or neutralize an external threat;

**RARITY:** can only be acquired by one or very few companies;

**INIMITABILITY:** costly to imitate, due to historical conditions, casual ambiguity or social complexity;

**ORGANIZATION:** a firm needs to be organized to capture the value.

| V | R | I | O | |
|---|---|---|---|---|
| ✓ | ✗ | | | Competitive Parity |
| ✓ | ✓ | ✗ | | Temporary Competitive Advantage |
| ✓ | ✓ | ✓ | ✓ | Sustainable Competitive Advantage |

| CAPABILITY | DESCRIPTION | VALUABLE | RARITY | INIMITABILITY | ORGANIZATION | RESULT |
|---|---|---|---|---|---|---|
| International Offices | Amongst the major players in most of the 15 countries (Europe and Asia) in which it operates. | *"We believe in the power of local"* – boosts client proximity. | Most players belong to international groups. | Expanding the geographical scope of commercial activity requires high CAPEX. | Group's support allied with local autonomy allows Ageas Portugal to exploit the resource. | **Competitive Parity** |
| Financial Situation | Strong financial situation. Numbers from 2019: - Combined ratio of 88% - Net income of 111M | Enables critical investments that ensure consistent success. | Main competitors also have a robust financial situation. | Not easily replicable as it is dependent on historical conditions and various skills/capabilities. | Financial stability assures insurer readiness to keep capturing value. | **Competitive Parity** |
| Well diversified portfolio | Broad range of services that goes beyond insurance by *"preventing, preparing, protecting, assisting and beyond".* | Reduces claims, boosts satisfaction, nurturing trusted relationships with the client. | Ageas and Fidelidade are the only players with various beyond insurance brands. | Enlarging the portfolio scope by entering new business lines involves high OPEX, time, effort. | The development of new businesses/ways of doing businesses proves that Ageas will continue to be a trusted partner. | **Sustainable Competitive Advantage** |

*Table 17:Tangible/Intangible Assets & Organizational Capabilities*

Legend: Tangible Assets | Intangible Assets | Organizational Capabilities | Criterion validated | Criterion not validated

# The sustainable competitive advantages identified were the diversified portfolio and the strong reputation of the company. The remaining resources were identified either as a temporary competitive advantage or competitive parity.

## D.2.2. Analysis | Internal Analysis | Resource-based View (II/II)

| RESOURCE | DESCRIPTION | VALUABLE | RARITY | INIMITABILITY | ORGANIZATION | RESULT |
|---|---|---|---|---|---|---|
| Efficient Operations | Long-term partnerships and innovation – part of Ageas DNA – are driven by technology. | Entails the organization to be agile and achieve cost efficiencies and economies of learning. | The only top player that highlights disruptive technology as a strategic objective. | Other companies may also strategically partner with technology-driven organizations. | Long-term partnerships with technology disruptors confirm the ability to reap the benefits. | **Temporary Competitive Advantage** |
| Empowered labour force | Skilled, experienced employees, from diverse backgrounds, but connected by great core values. | Excellent teamwork resulting from effective engagement of people. | Major players nurture a work environment that balances a healthy lifestyle with professionalism. | Changing people's mindsets and establish a renewed work environment is a long process. | The outstanding human resources management validates the company's ability to maintain excellent teamwork. | **Competitive Parity** |
| Omni-channel distribution | Seamless, integrated and consistent experience across all distribution channels – bank branches, brokers and agents, and mobile solutions. | Critical to meet customers' expectations and expand client's access to products. | Only the top insurers deliver an omnichannel customer journey. | Other companies can also start enlarging and integrating their distribution network. | Great customer experience is, in part, result of an omnichannel distribution network. | **Temporary Competitive Advantage** |
| Marketing Department | Marketing distinction – example: *Ageas Seguros* won the bronze trophy at the Gala of Communication Effectiveness Awards. | Innovative campaigns with effective trust messages boost brand engagement. | Only Fidelidade and Tranquilidade have Marketing Departments achieving Ageas' level. | Other companies may also improve their current marketing capabilities | The client's engagement achieved in 15 years reveals the excellence of Ageas' marketing department. | **Temporary Competitive Advantage** |
| Strong Reputation (customer-centricity) | Customer-centricity - *"We exist for our customers."* – is the ultimate goal of all capabilities and results in a strong reputation. | By delivering a meaningful and emotional experience to its customers, Ageas nurtures brand trust and reputation. | Most insurers follow a customer-centricity approach but only top players can successfully implement it. | Reaching the maturity stage of customer-centricity strategy is a consistent and continuous path and prestige is hard to replicate. | Ageas Portugal success reflects the ability of the company to reap the benefits of placing customers at the core of its business. | **Sustainable Competitive Advantage** |

*Table 17 (continuation): Tangible/Intangible Assets & Organizational Capabilities*

***Sources**: Resource Based View Model, Team Based, Ageas Group, Ageas Portugal, Fidelidade, Tranquilidade, Allianz*

# Ageas should develop strategic options, by leveraging on its strengths together with the market opportunities to tackle the main threats and overcoming its weaknesses.

## D.2.3. Analysis | Internal Analysis | SWOT and TOWS

Further Detail: Appendix 7

| | | Internal Environment | |
|---|---|---|---|
| | | **Strengths (S)**<br>**(S1)** Solid client base<br>**(S2)** Robust financial situation<br>**(S3)** Technology and innovation driven culture<br>**(S4)** Strong brands and partnerships<br>**(S5)** Great customer experience | **Weaknesses (W)**<br>**(W1)** Lack of specialization and technical expertise on cybersecurity<br>**(W2)** High level of commitment of the company<br>**(W3)** Scarcity of data inside the company |
| External Environment | **Opportunities (O)**<br>**(O1)** Digitalization has led to a brisk evolution of cyber risks<br>**(O2)** Mismatch between clients' needs and insurers' offers<br>**(03)** Evolving regulations catalyze improvements of cyber risk awareness and mitigation | **Strengths + Opportunities**<br>(S1&S4 + O1&O2) Provide a differentiated cyber insurance offer for both current and new customers<br>(S3 + O2) Cyber risk intrinsically related to technology and digitalization, embracing the company's culture<br>(S4 + 03) Strong brands, crucial to attract new customers that arise from increasing cybersecurity regulations | **Weaknesses + Opportunities**<br>(W2 + O3) Increasing regulation may lead to a rise in available external data for the company<br>(W1 + O2) Investment in specialization and expertise on the company will help to create a solution tailored to customers' needs |
| External Environment | **Threats (T)**<br>**(T1)** Influx of new entrants due to high profitability and growth potential<br>**(T2)** Alternative coverage solutions disrupting the industry<br>**(T3)** Short supply of skilled workers<br>**(T4)** Limited application of standard actuarial techniques | **Strengths + Threats**<br>(S2&S4 + T1&T2) Acquisition of smaller competitors may be an option to decrease direct and indirect competition<br>(S2 + T3&T4) Financial strength crucial to invest in skilled workers and partner with the best technology providers<br>(S3 +T4) The culture of the company will ease the adoption of the latest actuarial techniques | **Weaknesses + Threats**<br>(W1+T1&T2) New entrants and alternative solutions, when specialized in cybersecurity, impose a threat to the company;<br>(W3 + T3&T4) The internal lack of data allied to the shortage of workers and limited actuarial techniques may hamper the entry is this market |

*Figure 19: SWOT and TOWS Analyses*

***Sources**: Grupo Ageas Portugal , Insource Journal, AON, Deloitte, PORDATA, IBM, Munich RE, Team Based*

# The first step in the strategy formulation was to test the hypothesis using qualitative (in-depth interviews) and quantitative (surveys) investigation methods to both segments (B2B and B2C).

## E.1. Strategy Formulation | Investigation Methods

Further Detail: Appendix 9

Further Detail; Appendix 10

### Main Hypothesis Tested in In-depth interviews and Surveys

- Test awareness to cyber risk; - Test the level of readiness; - Test product features

- Test distribution channels; - Test willingness to pay and willingness to buy

### In-depth Interviews

In the **B2B segment**, IT managers or managers of four companies in four different industries (included in the most affected ones) were interviewed.

In the **B2C segment** ten individuals from four target groups were chosen: married with children, married with no children, single with children and single with no children. The name of Ageas was never disclosed during these interviews. The interviews had a duration of **30-45 minutes** and focused on the following topics: **(1)** Awareness of cyber risks; **(2)** Victim (or not) of cyber risks; **(3)** Cybersecurity measures implemented and **(4)** Interest on cyber insurance (reasons for having/not having insurance; most wanted features; preferred distribution channels for purchase and willingness to buy in the future).

### Surveys

**B2B**

**(1) Firmographics:** no. of collaborators, industry, revenues; **(2) EAR[1] questions:** level of dependency on IT, assessment and mitigation measures, previous cyber attacks (reasons, motivations and consequences); **(3) Companies with cyber insurance:** main features, selection criteria, distribution channels used and pricing; **(4) Companies without cyber insurance:** reasons for not purchasing, WTB in the future, most wanted features, preferred distribution channel and WTP.

**B2C**

**(1) Demographics:** age, gender, region, occupation, highest degree, no. of children, annual Income); **(2) TAR[2] questions:** level of dependency on the internet, security in devices and previous cyber attacks (most common, consequences and objectives); **(3) Individuals with cyber insurance:** main features, selection criteria, distribution channels used and pricing; **(4) Individuals without cyber insurance:** reasons for not purchasing, WTB in the future most wanted features, preferred structure and distribution channel and WTP.

[1] Exposure, Awareness and Readiness; [2] Tech-savviness, Awareness and Readiness

***Sources**: Team Based, In-Depth Interviews, Surveys*

# Upon four in-depth interviews, most companies claimed lack of awareness and necessity as the main reasons for not having cyber insurance, whereas eight of the ten individuals interviewed showed willingness to buy the product.

## E.2. Strategy Formulation | In-depth Interviews: B2B & B2C

Further Detail: Appendix 12

### B2B

**Methodology**

| | Name | Industry |
|---|---|---|
| JCDecaux | JcDecaux Portugal | Professional, Scientific and Technical Services |
| Europa | Clínica Europa – Grupo Joaquim Chaves | Healthcare and Social Assistance |
| IFA | IFA - Instituto de Formação Aeronáutica | Educational Services |
| Rozès | Rozès, S.A. | Manufacturing |

*Table 18: Methodology In-depth interviews B2B*

**Key Insights**

**Most frequent Incidents**

- Phishing; Malware; Ransomware

**Main consequences**

- Business interruption;
- Reputational costs

**Preventive measures**

- GDPR compliance plan
- Disaster recovery plan

**Protective measures**

- Employee education;
- IT security systems;
- Password policies;
- Back-ups

**Cyber Insurance**

- Only 1/4 companies has cyber insurance
- 3/4 lack awareness and necessity to the product;
- Features: coverage allied to prevention/ protection;
- Preferred Channel: brokers

### B2C

**Methodology**

| Group | Woman | Men | Total |
|---|---|---|---|
| **Married with children** | 4 | 1 | 5 |
| **Married with no children** | 1 | 1 | 2 |
| **Single parents** | 1 | 0 | 1 |
| **Singles with no children** | 2 | 0 | 2 |

*Table 19: Methodology In-depth interviews B2C*

**Key Insights**

**Most frequent Incidents**

- Phishing;
- Identity Theft

**Main consequences**

- Loss of Information;
- Financial Losses

**Most frequent measures**

- Anti-virus protection;
- Parental control

**Cyber Insurance**

No interviewee had cyber insurance

Main reasons:

- Lack of awareness (8/10)
- Lack of necessity (2/10)

**Willingness to buy in the future**

- 8/10 are willing to buy cyber insurance;
- Most interviewees would like to have coverage allied to pre-breach services;
- Preferred channels: brokers and stores

***Sources**: In-Depth Interviews*

# The answers of 43 respondents were analysed and revealed that, on average, 1 out of 3 companies have suffered a cyber attack and half of those were attacked more than once.

## E.3.1. Strategy Formulation | Surveys: B2B (I/II)

**Further Detail: Appendix 13**

**Methodology** In order to better evaluate SMEs' needs, part of the questions were grouped into two characterization variables: Exposure and Awareness & Readiness.

### Key Insights: Exposure

**Previous victims of cyber attacks**

- Victims: 33% (out of which, 57% were attacked more than once);

**Digital Platforms**

| | |
|---|---|
| Website | 88% |
| Social Media | 67% |
| E-commerce | 35% |
| Marketplace | 9% |

**Motivations of the attacks**

- Cyber Extortion: 64%
- Cyber Espionage: 14%

**Dependency on IT/OT**

Scale of 1-10:

Median: 8 | Average: 7.6

**Major Consequences**

| Most Feared | | Actual | |
|---|---|---|---|
| 1 | Business Interruption | 1 | Business Interruption |
| 2 | Asset Losses | 2 | Asset Losses |
| 3 | Compliance costs | 3 | Employee Motivation |
| 4 | Reputational Damage | 4 | Compliance Costs |
| 5 | Employee Motivation | 5 | Reputational Damage |

### Key Insights: Awareness & Readiness

**Organisational Structure**

| | |
|---|---|
| IT Department | 51% |
| IT Security Area | 14% |
| DPO | 9% |
| CISO | 7% |

*Graph 7: Organisational Structure*

**Incidents recognized**

- Median: 5 (out of a list of 8)

- Virus
- Malware
- Hacking

**Risk Assessment Measures**

- Vulnerability Diagnosis: 58%
- Compliance Evaluation: 56%
- Security Tests: 44%

**Risk Mitigation Measures**

- Data Back-ups: 88%
- Network Access Control: 86%
- Software Updates: 72%

**Cyber Incident Management**

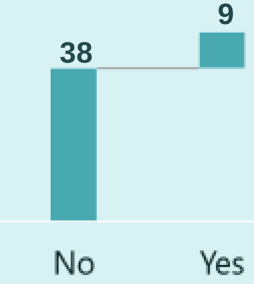
| Internally | Cybersecurity Partners | Contracting Suppliers |
|---|---|---|
| 42% | 33% | 8% |

*Figure 20: Survey Key Insights (B2B)*

### SAMPLE COMPOSITION

- **Number of Answers: 47**

Companies with cyber insurance policies:




**4** out of **9** **not willing to replace** their current policies

The key insights only contemplate: **43** answers

**Industries**

| | | |
|---|---|---|
| Most Affected Sectors[1] | 79% | **Most frequent:** Accommodation; Wholesale Trade; Manufacturing; Transportation & Warehousing |
| Least Affected Sectors[1] | 21% | |

**No. Employees**

| < 10 | 10-250 |
|---|---|
| 2% | 98% |

**Job Roles**

**Most frequent:**
- CTO/ IT Manager
- CEO

*Figure 21: Sample Composition (B2B)*

***Sources**: Surveys*

# Surveyed companies have expressed their interest in having pre-breach features (risk assessment and mitigation) included in their cyber insurance, besides the covered costs.

## E.3.1. Strategy Formulation | Surveys: B2B (II/II)

Further Detail: Appendix 13

### Key Insights: Customers' Needs & Preferences on Cyber Insurance

**W/ Cyber Insurance**

**Motivations to buy[1]**

- Company's Size: 40%
- Brand Value: 40%
- Digital Transformation: 40%
- Occurrence of an attack: 40%
- Sensitive Information: 20%

**Key Factors in Selection** [by order of preference]

1. Coverage
2. Trust in Insurer
3. Price
4. Additional Services
5. Application Form

**Satisfaction Level**

- "Satisfied": 100%

**Application Form** [points awarded]

| | | |
|---|---|---|
| Extension | 3 | 3 |
| Language | 3 | 5 |

Avg. (scale of 1-5)

**Distribution Channels**

- The enterprise contracted an agent: 3/5

**Access to a Risk Assessment Tool**

- Yes: 1/5
- No: 4/5

**No Cyber Insurance**

**Reasons for not having cyber insurance[1]**

- Lack of knowledge: 58%
- Lack of necessity: 26%
- Inaccessible pricing: 16%
- Limited coverage: 13%
- Complex AF[2]: 3%

**Most wanted cyber insurance features**

Risk Assessment
- Vulnerability Diagnoses
- Pen Tests
- Compliance Evaluation

Coverage (costs)
- Assets recovery
- Business Interruption
- Fraud/Theft

Risk Mitigation
- Employee Training
- Data Back-up
- Periodic Monitoring
- Incident Response Plan

Assistance services
- Technical Assistance
- Legal Assistance

**Distribution Channels**

- Specialized Agent: 66%
- General Agent: 11%
- Online: 5%

*Figure 22: Customers' Needs & Preferences (B2B)*

### Key Takeaways

1. Approximately 1 out of 3 companies suffered a cyber incident;
2. The most feared consequences are business interruption, asset losses and costs due to non-compliance with regulations/law, but the most recurrent consequences include employees' underperformance and demotivation;
3. SMEs have yet a low level of awareness, with only 14% of enterprises including an IT Security Area in their organizational structure;
4. However, 19% of companies have already purchased cyber insurance. The most wanted coverage features are assets recovery, business interruption and fraud/theft costs.

[1]Respondents could select more than one answer. Percentages are given by: total of selections/no. of respondents; [2]AF: Application Form

***Sources**: Surveys*

# The results of the survey directed to individuals confirmed their increasing dependence on technology and the yet low level of awareness and readiness to cyber risks.

## E.3.2. Strategy Formulation | Surveys: B2C (I/II)

Further Detail: Appendix 13

**Methodology**

To better evaluate people's needs, part of the questions were grouped into two characterization variables:

Tech-Savviness and Awareness & Readiness.

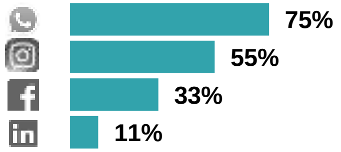
### Key Insights: Tech-Savviness

**Level of internet dependency**

Scale of 1-10:

Median: 7 | Average: 6.6

**Most Used Social Media**

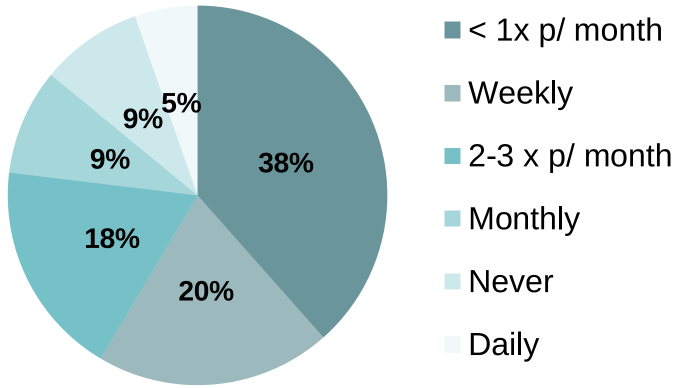



Graph 8: Most Used Social Media

**Financial Operations Online**

- 89% of the surveyed people do financial operations online

**Posting on Social Media**




Graph 9: Posting frequency on Social Media

### Key Insights: Awareness & Readiness

**Previous victims of cyber attacks**

- Victims: 16% (out of which, 36% were attacked more than once)

**Perceived Level of Threat**

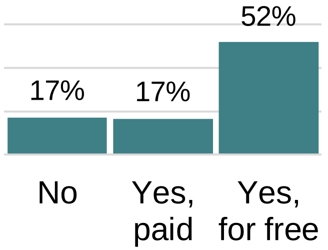
Scale of 1-10:

Median: 4 | Average: 4.7

**Major Consequences**

| | Most Feared | | Actual |
|---|---|---|---|
| 1 | Financial | 1 | Loss of Time |
| 2 | Psychological | 2 | Financial |
| 3 | Reputational | 3 | Psychological |
| 4 | Loss of Time | 4 | Reputational |

**Security in Devices[1]**




Graph 10: Devices security

| | | |
|---|---|---|
| 1 | Anti-virus | 53% |
| 2 | Data back-ups | 16% |
| 3 | VPN | 13% |
| 4 | Multifactor authentication | 12% |
| 5 | Data encryption | 5% |
| 6 | Other | 1% |

Figure 23: Survey Key Insights (B2C)

### SAMPLE COMPOSITION

- **Number of Answers: 525**

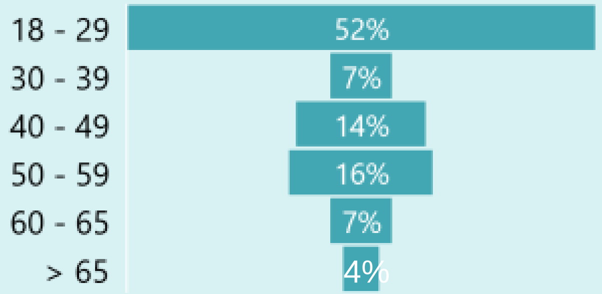
**Gender Distribution**

60% 40%

**Parents with underage children**

17%

**Age Distribution**




Graph 11: Sample Age Distribution

**Region Distribution**

- North: 2%
- Centre: 13%
- Metropolitan Area of Lisbon: 73%
- Alentejo: 4%
- Algarve: 2%
- Açores: 6%
- Madeira: 0%

Figure 24: Sample Composition (B2C)

[1]The remaining 14% answered "Do not know"; ***Sources***: *Surveys*

# The majority of people were not aware of cyber risk insurance offers, but when faced with the possibility of acquiring it, the general preference was towards an add-on and modular policy with pre-breach services.

## E.3.2. Strategy Formulation | Surveys: B2C (II/II)

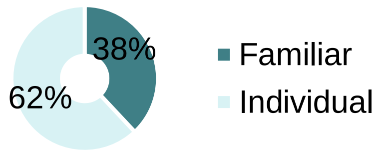
Further Detail: Appendix 13

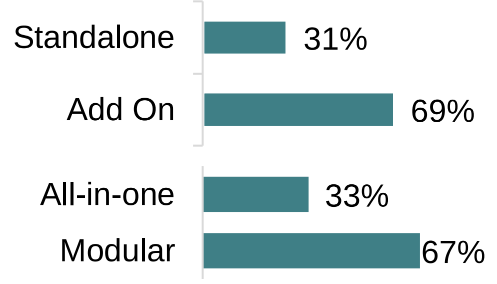
### Key Insights: Customers' Needs & Preferences

#### Reasons for not having cyber insurance[1]

- Lack of knowledge: 78%
- Lack of necessity: 21%
- Inaccessible pricing: 6%
- Limited coverage: 3%
- Other: 2%

#### Structure of the Cyber Insurance



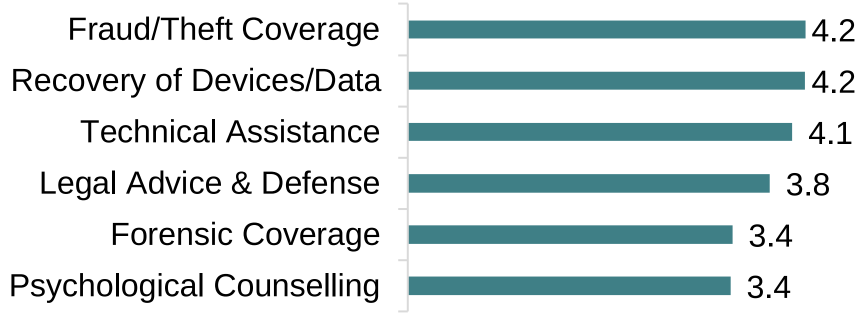




*Graphs 12, 13 and 14: Cyber Insurance Structure*

#### Most wanted cyber insurance features

**Coverage (costs)**

[average points awarded on a scale of 1-5]




*Graph 15: Average points awarded to each cyber insurance coverage feature*

**Risk Mitigation**

[by order of preference]

| | |
|---|---|
| 1 | Anti-virus |
| 2 | Data back-ups |
| 3 | Encryption techniques |
| 4 | Multifactor authentication |
| 5 | VPN |
| 6 | Parental control online software |

#### Distribution Channels

- Online: 36%
- Physical Store: 33%
- Agent: 17%
- Mobile: 14%

*Figure 25: Customers' Needs & Preferences (B2C)*

### Key Takeaways

1. Approximately 9 out of 10 people do financial operations online;
2. 16% of people have suffered a cyber incident; The most feared consequences are financial, psychological and reputational damages, but the most recurrent consequence is loss of time;
3. Individuals and families have yet a low level of awareness, evaluating their perceived level of threat with 4.7 points out of 10.
4. However, 69% of people have already paid or free cybersecurity in their devices.
5. The most wanted cyber insurance coverage features are fraud/theft cost, devices/data recovery and technical assistance.

[1]Respondents could select more than one answer. Percentages are given by: total of selections/no. of respondents

***Sources***: *Surveys*

# Differentiation strategy should underpin Ageas' strategic decisions. To develop a value proposition able to sustain a long-term competitive advantage, the team applied the STP model and an adapted version of the 7Ps marketing mix.

## E.4. Strategy Formulation | Overall Strategy

**Source of Competitive Advantage**

| Competitive Scope | Cost | Differentiation |
|---|---|---|
| Narrow | **Cost Focus** When a firm seeks a cost advantage in its target segments | **Differentiation Focus** When a firm seeks differentiation in its target segment |
| | **Stuck in the Middle** | |
| Broad | **Cost Leadership** When a firm seeks out to become the low cost producer in its industry | **Differentiation** When a firm seeks out to be unique in its industry along some dimensions widely valued by customers |

Figure 26: Porter's Generic Strategies

Considering the internal and external analysis, the team proposes Ageas to follow a **Differentiation strategy** to explore the **untapped demand** and *"deliver a **meaningful** and emotional experience"* by **addressing the dimensions** that restrain customers from adopting cyber insurance.

**Segmentation**

*"Group customers based on similar needs. Profile each segment."*

**Clustering:** weighted variables were incorporated in broader dimensions.[1]

**Targeting**

*"Assess **attractiveness** of each segment. Select segments to target."*

**Differentiated marketing:**

Target several attractive segments, by offering tailored solutions.[1]

**Positioning**

*"Define **value proposition** for target segments. Develop an **action plan**."*

Figure 27: STP & Targeting Strategy Models

**Value Proposition**

*Marketing Mix – 7Ps (adapted)*

**Target Clusters**

- Profile target clusters needs/preferences

**Product**

- Coverage
- Type and Structure

**Underwriting**

(Processes)

Solutions to control cyber evolving risks.

**"Go-to-Market" Plan**

(Place, Promotion, People, Physical Evidence)

- Ageas' brands
- Distribution channels
- Engagement strategies
- salesforce incentives

**Pricing Concept**

(Price)

Roadmap for adequate pricing (considering cost, competition and customer dimensions)

Figure 28: Adapted Marketing Mix – 5Ps

**Action Plan**

Actions – Responsible Departments – Timeline

[1]Further explanation on Rationale of Recommendation 1) and 5) – Afonso Gomes; ***Sources***: *Team-based, Harvard Business School*

# Leveraging on customer insights, the team segmented, profiled and targeted the most attractive ones within SMEs and families. The positioning statements guided the development of a differentiated value proposition.

## E.5. Strategy Formulation | STP Model

| For SMEs | STP Model | For Families |
|---|---|---|
| Segment businesses according to: **exposure** and **awareness –** conditionate risk mitigation needs and communication approach. The risk assessment tool and vulnerability analysis will profile SMEs by firmographics and behavioural variables. | Segmentation | Segment families according to: **tech-savviness** and **children or not –** conditionate features' needs and communication approach. The risk assessment tool will profile families by demographics and Norton's safety panel will empower ongoing CRM. |
| Attractiveness was analysed by size: (1) micro – low financial flexibility; (2) large – red ocean (cybersecurity providers' focus), highly risky. Hence, the client agreed on leaving these segments out of scope and **target all SMEs** – higher return for lower risk. | Targeting | Inherent to cyber nature, this insurance is more directed to highly digital dependent people. The driver of kids' protection entails great potential to parents clusters. Overall, low tech people – a shrinking segment – were the only excluded. |
| *"For **SMEs** that value clients and employees safety, Ageas CyberShield is the only insurance offering **flexible tailored solutions,** including **OutThink's targeted employee training** along with comprehensive pre- and post-breach services."* | Positioning Statement | *"For people who value their family's online safety, Ageas CyberShield is the only insurance offering **flexible tailored solutions**, including **Norton's 360 protection** along with comprehensive legal coverage and assistance."* |

***Sources***: *Team-based, Harvard Business School*

# The team proposes the exploitation of untapped demand by addressing supply-demand gap drivers. Hence, Ageas will be able to ”deliver a meaningful and emotional experience”, while controlling claims and risks.

## E.6. Strategy Formulation | Rationale of the Value Proposition

**Supply-demand gap drivers:**

- Lack of awareness;
- Lack of tailored and transparent solutions;
- Absence of specialized brokers;
- Underwriting challenges;
- Overpriced policies.

Ageas should adopt a **Differentiation Strategy** to explore **untapped demand** and “*deliver an emotional and meaningful experience*”, while **controlling claims and risks**.

**Expected Impact**

- Raise awareness A
- Boost product adoption B
- Dedicated and skilled salesforce C
- Reduce claims frequency and severity D
- Adequate pricing E

*Note: KPIs on Individual Recommendations*

| Target Customer B | Product - Coverage B D |
|---|---|
| Cluster SMEs according to the most relevant variables to determine their needs, enabling **tailored solutions**. | **Differentiate** (PoD) and adopt an **universal language** (ENISA framework). SMEs: comprehensive offer (PoP) and OutThink’s targeted **employee training** (PoD); 24h access to an automated **vulnerability analysis app**. Families: Norton 360 multidevice **protection** (PoD) and comprehensive post-breach services (PoP); 24h access to a **safety panel**. |
| **Product – Type & Structure B** | **“Go-to-Market” Plan A B C** |
| Offer flexible coverage that allows clients to build a **tailored policy** to their needs/preferences. SMEs: standalone policy; Families: standalone or add-on policy. Both: **multiple plans** to be complemented with **optional modules**. | Design a **customer journey** map as a guide; rank Ageas’ **brands** to place CyberShield; select **distribution channels**; develop **awareness** and **engagement** strategies and facilitate learning resources and an incentive program to **salesforce**. |
| **Underwriting D E** | **Pricing E** |
| Design **solutions** to overcome underwriting challenges to **control risks** of tailored and comprehensive cyber solutions. | Incorporate **customer, cost** and **competition** orientation to commercialize a premium offer at a competitive price. |

*Table 20: Overview of Recommendations*

***Sources**: Team-based*

# Prioritization of recommendations considers the potential impact and the level of effort in terms of planning and investment resources; 8 quick-wins and 5 major projects are grounded on the 5 pillars of an efficient value proposition.

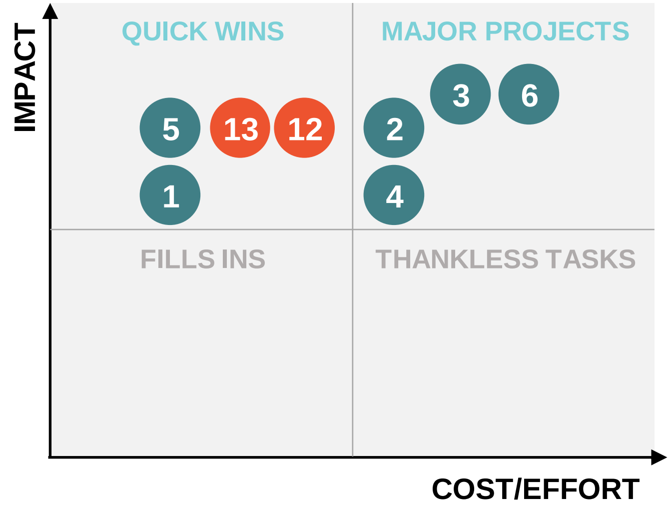
## F.1. Recommendations | Overview and Action-Priority Matrix

| | RECOMMENDATIONS[1] | TARGET | PRODUCT | GO-TO-MARKET | UNDERWRITE | PRICE |
|---|---|---|---|---|---|---|
| 1 | Target selected cluster segments | ✓ | | | | |
| 2 | Offer comprehensive pre-breach services (PoP) | | ✓ | | | |
| 3 | Offer targeted employee training (PoD) | | ✓ | | | |
| 4 | Offer comprehensive post-breach services | | ✓ | | | |
| 5 | Frame the product as standalone and modular | | ✓ | | | |
| 6 | Develop an efficient “go-to-market” plan | | | ✓ | | |
| 7 | Target selected cluster segments | ✓ | | | | |
| 8 | Offer comprehensive pre-breach services (PoD) | | ✓ | | | |
| 9 | Offer comprehensive post-breach services (PoP) | | ✓ | | | |
| 10 | Frame the product as add-on/standalone and modular | | ✓ | | | |
| 11 | Develop an efficient “go-to-market” plan | | | ✓ | | |
| 12 | Design solutions to overcome underwriting challenges | | | | ✓ | |
| 13 | Adopt a comprehensive pricing concept | | | | | ✓ |

B2B B2C B2B & B2C (Operational)

*Table 21: Impact of the recommendations on the marketing mix (adapted) framework*

### ACTION PRIORITY MATRIXES



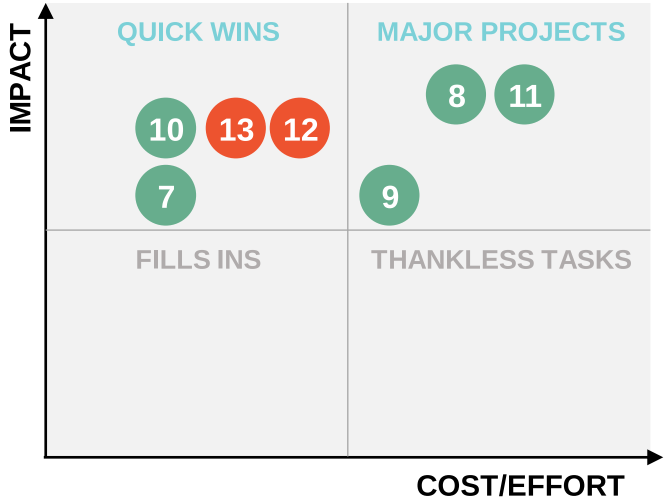




*Figure 29: Action-priority matrixes of recommendations*

[1]**Note:** *Afonso Gomes: 1), 5), 7), 10), 13) Madalena Sangalho: 6), 11), 12) Raquel Brites: 2), 3), 4), 8), 9)*

**Sources**: *Team-based*

# The action plan for the implementation of recommendations comprises 5 steps and it is predicted to take one and a half years; it culminates in the launch of Ageas cyber risk value proposition for SMEs and families – CyberShield.

## F.2. Recommendations | Action Plan

| NR. | Task | Responsible Department | 2021 Q1 | 2021 Q2 | 2021 Q3 | 2021 Q4 | 2022 Q1 | 2022 Q2 |
|---|---|---|---|---|---|---|---|---|
| **1.** | **REVIEW OF VP** | | | | | | | |
| 1.1. | Case Studies | Strategy, Innovation and Sustainability | | | | | | |
| 1.2. | Adjust Value Proposition & Approval of Limits and Exclusions | Technical & Offer | | | | | | |
| 1.3. | Approval of Limits, Exclusions & Requisites | Technical & Offer | | | | | | |
| 1.4. | Test and Validate (Pilot Project) | Technical & Offer | | | | | | |
| **2.** | **PARTNERSHIP – NORTON, LAZARUS & OUTTHINK** | Partnership – Due Diligence Team | | | | | | |
| 2.1. | Contact Norton and negotiate model of collaboration | Partnership | | | | | | |
| 2.1. | Close negotiations with Lazarus | Technical & Offer & Due Diligence Team | | | | | | |
| 2.2. | Contact OutThink and review labour code legislation | Partnership & Legal Department | | | | | | |
| 2.3. | Negotiate model of collaboration with OutThink | Due Diligence Team | | | | | | |
| **3.** | **OUTSOURCE CONTRACTS** | Partnership - Due Diligence Team | | | | | | |
| **4.** | **DEVELOP RESOURCES & TOOLS** | | | | | | | |
| 4.1. | Risk Assessment Tool | IT & Underwriting | | | | | | |
| 4.2. | Other resources (videos, learning materials, etc.) | Technical & Offer, HR & Marketing | | | | | | |
| **5.** | **PRE-LAUNCH** | | | | | | | |
| 5.1. | Prepare brokers and agents (introduce the insurance & tools, explain incentive programs, etc.) | HR & Distribution | | | | | | |
| 5.2. | Organize Webinars | Marketing Department | | | | | | |
| 5.1. | Contact Retail Stores | Partnership | | | | | | |
| 5.2. | Social Media Marketing & contact influencers | Marketing Department | | | | | | |

*Table 22: Action Plan of Recommendations*

Disclaimer:

The project concerns the development of a cyber risk value proposition. Hence, it is logical to present the consolidated action plan of the recommendations that culminates in the launch of CyberShield.

**Legend:**

- SMEs & Families
- Families
- SMEs

***Sources**: Team-based, Ageas Portugal*

# The team identifies the main risks to be addressed in further research. The key challenges faced throughout the project were the scarcity of available data and the complexity of the proposed topic – cyber insurance.

## G. Risks, Further Research and Limitations

*Table 40: Risks and Further Research*

| | Risks | Further Research |
|---|---|---|
| **Target Customer** | Inadequacy of characterization variables to determine segments' needs and preferences. | Case studies will disclose valuable customer insights. Moreover, the vulnerability analysis app and safety panel (24h access) will empower continuous collection and treatment of the client's data, which enhances market segmentation. |
| **Cyber Product** | Unfeasible partnerships (OutThink and Norton); High price sensitivity hampering the delivery of flexible and differentiated solutions. | The team identified other potential strategic partnerships; case studies will enable an adjustment value proposition; the awareness and engagement strategies will also help customers to perceive the value of Ageas' differentiated offer. |
| **Go-to-Market Plan** | Unexpected response of salesforce; low engagement (awareness tools and social marketing); high demands from suggested influencers. | The team identified other potential social media collaborations; Marketing Department may conduct further studies to disclose more suitable content to post/publish; Human Resources Department may improve training and incentives programs. |
| **Underwriting and Pricing** | The inherent recency and evolving nature of cyber risks amplify (re)insurers' underwriting and pricing uncertainties. | Although the scope of the project excluded the underwriting process and actuarial models, Ageas' skilled teams will address to a greater extent these topics – reviewing and aligning the proposed limits, exclusions and requisites. |

### Limitations and Challenges

**(1) Scarcity of available data** about the cyber insurance industry. Lack of quantitative data (premiums and claims) constrained the market potential assessment and limited the forecast of profitability indicators. The lack of commonality of language and the evolving nature of cyber risks hampered the team's collection and treatment of qualitative data.

**(2) Complexity of the Topic**: Insurance subjects are extremely complex, namely underwriting and pricing. Cybersecurity is a highly technical topic distant from the teams' academic field. Hence, the cyber insurance project implied extensive preliminary research.

**(3) B2B:** The collection of insights about SMEs' needs and preferences (surveys) was a major challenge.

***Sources**: Team-based*

A Work Project, presented as part of the requirements for the Award of a Master's degree in Management from the Nova School of Business and Economics.

# CONSULTING PROJECT WITH THE TOPIC: "AGEAS CONSULTING FIELD LAB ON A CYBER RISK VALUE PROPOSITION – GO-TO-MARKET PLAN AND OVERCOMING UNDERWRITING CHALLENGES"

MADALENA MADEIRA SANGALHO | 29203

Work Project carried out under the supervision of:

Professor Constança Monteiro Casquinho

04.01.2021

# Mapping the customer journey guides the design of a customer-centric “go-to-market” plan, in which the ultimate goal is to deliver an omnichannel superior experience to increase customer lifetime value.

## F.5. Recommendations B2B | Develop an efficient “go-to-market” plan (I/IV)

### VALUE CREATION

To customers: The marketing efforts demystify the complexity of the value proposition; in particular, the risk assessment tool allows SMEs to simulate potential losses from cyber risks and case studies reduce clients’ uncertainty about the value of cyber insurance.

To Ageas: The delivery of an omnichannel customer experience will boost marketing reach: the raise of awareness and engagement will be translated into higher conversion rates and salesforce incentives will enhance their marketing approaches and thus, increase the number of new policies per agent.

### DESCRIPTION

Map the **customer journey** as a guide to an efficient “go-to-market” plan.

- Place**:** Propose (by ranking) the most appropriate **Ageas’ brands** to commercialize CyberShield; select **distribution channels** according to clients’ preferences and insurance characteristics.
- Promotion**:** Develop **awareness and engagement strategies** to communicate the real value of the product.
- People**:** Facilitate **learning materials** and organize an **incentive program** to salesforce – brokers and agents (including remuneration and training).
- Physical Evidence: In this industry, as the service is the only experience after the delivery, insurers help potential customers to perceive the value of the policy purchase by providing **case studies**.

**Consumer Buying Process:** *“All the experiences in learning, choosing, using, and even disposing of a product.”[1]*

**Place:** *“All the company activities that make the product or service available to target customers.”[2]*

**Promotion:** *“Activities that communicate the product or service and its merits to target customers and persuade them to buy.”[2]*

**People:** *“All human actors who play a part in service delivery and thus influence the buyers’ perceptions (…).”[3]*

**Physical Evidence:** *“(…) any tangible components that facilitate performance or communication of the service.”[3]*

[1]Kotler & Keller (2012); [2]Kotler et al (2005); [3] Zeithaml & Bitner (2003) ***Sources**: Team-based*

# The complex underwriting constrains the placement of CyberShield within Ageas' portfolio; surveys, interviews and research insights reflect SMEs' lack of awareness and engagement, partially driven by salesforce expertise absence.

## F.5. Recommendations B2B | Develop an efficient "go-to-market" plan (II/IV)

### RATIONALE (continuation)

#### Omnichannel Customer Experience Journey (CEJ)

- **Ageas' customer-centricity:** *"We exist for our customers."*
- Advantages of **superior customer experience** for insurers:

1. **Grow faster:** 2-4x more in new businesses;
2. **More profitable:** 30% higher profitability;
3. **Higher retention:** satisfied customers are 80% more likely to renew their policies.

**Omnichannel approach:** multichannel and focused on delivering a seamless customer experience, regardless of the client's journey.

**Customer journey mapping** provides a common vision to all departments involved in the delivery of a superior customer experience. Thus, it guides a customer-centric go-to-market plan

#### Qualitative Assessment of Ageas' Brands to commercialize CyberShield

| Ageas' Brands | ageas seguros | OCIDENTAL SEGUROS | SEGURO DIRECTO grupo ageas |
|---|---|---|---|
| 👍 | • Benchmark evidence<br>• Strong Brand Image<br>• Personalized experience<br>• Large client base | • Strong digital presence<br>• Personalized experience<br>• Large client base | • Strong digital presence<br>• Possibility to leverage portfolio |
| 👎 | • Lack of digital presence | • Benchmark evidence | • Complex underwriting process<br>• Misfit with the brand image |

*Table 31: Ageas brand's pros and cons to sell CyberShield*

#### Customer distribution channels preferences:

**Survey Insights:** SMEs without **insurance**: specialized agent (66%), general agent (11%), online channels (5%), SMEs **with insurance**: 3 out of 5 contacted an agent to adopt the cyber policy

#### Awareness, Engagement and Low Market Penetration

- **Survey Insights:** Reasons for not having insurance: **lack** of **knowledge** (58%), **lack** of **necessity** (26%). Relevancy of a **risk assessment tool** – median of 4 (scale of 1-5). Only 1 out of 5 SMEs had access to one.
- The **lack of SMEs' cyber risk awareness** was reinforced by all experts during the interviews.
- **Agents'/Brokers' lack of expertise** about cyber risks constitutes is a major driver of **low market penetration.**[2]

[1]Ageas Portugal; [2]McKinsey; [3]Deloitte;

***Sources**: Ageas Portugal McKinsey, Team-based, Ageas Portugal, Surveys, Deloitte*

# Ageas Seguros and Ocidental online channels should promote CyberShield for follow-up personal selling through agents and brokers. Case studies and articles help potential clients to perceive the value of Ageas' cyber insurance.

## F.5. Recommendations B2B | Develop an efficient "go-to-market" plan (III/IV)

### RATIONALE (continuation)

**Best Practices: (1)** Most insurers provide **awareness resources** (e.g. case studies and articles); **(2)** Caravela organized – in November 2020 – a webinar to present its cyber insurance and **(3)** Fidelidade and Innovarisk facilitate a free risk assessment tool.

### RECOMMENDATION

*Figure 36: Omnichannel Customer Experience Journey (CEJ)*

| | Awareness | Consideration | Purchase | After Sales Services | Make a Claim |
|---|---|---|---|---|---|
| Internet | Online search | Risk assessment tool | | Awarded Feedback | Ask for Rating Review |
| Agent/Broker | Webinar Invitation | Multimedia Demo | Buy through agent/broker | Ongoing services:<br>- Vulnerability Analysis & Resolution<br>- Employee Education<br>- Technical Assistance | Ask for Rating Review |
| Retail Branch | Webinar Invitation | Request further information | Buy through agent/broker | | |
| Bancassurance | Millennium Channels | | Buy through agent/broker | | Report claim and activate coverage & assistance services |
| Call center | | | | | |

Legend: Customer X; Customer Y

**Note:** Omnichannel approach: at any stage, the customer can switch to a different channel.

**Recommended Brands:**

1. ageas seguros
2. OCIDENTAL SEGUROS
3. SEGURO DIRECTO grupo ageas[1]

**Distribution Channels:**

- Brokers/Agents – Purchase
- Online – Promotion

**Case Studies and Articles**

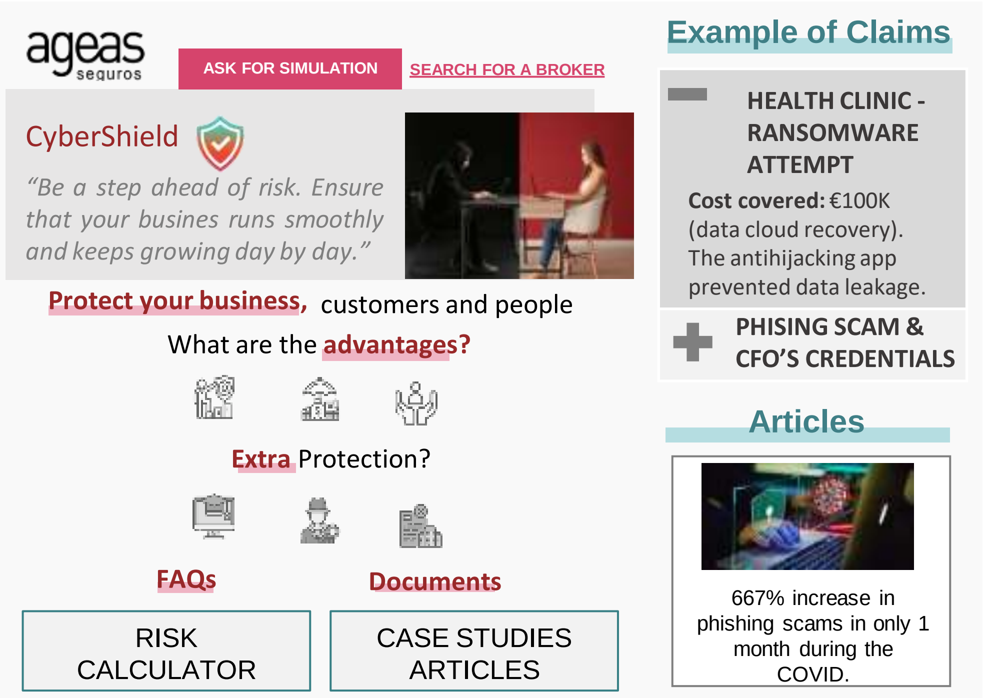



*Figure 37: Overview of main webpage and case studies & articles (website)*

[1] Due to the underwriting challenges, the team proposes Ageas to disregard, for now, Seguro Directo.

***Sources**: Team-based, Caravela, Fidelidade, Innovarisk, Ageas Portugal*

# The risk assessment tool and webinars raise awareness and engagement through an interactive first contact. The video demo, learning resources, attractive commissions and career opportunities empower the salesforce.

## F.5. Recommendations B2B | Develop an efficient "go-to-market" plan (IV/IV)

Further Detail: Appendix 30

## RECOMMENDATION

### Risk Assessment Tool:

**1. KEY INFORMATION**
- Size of the company
- Industry
- Operating Revenues
- No. of users of digital assets.

**2. ADDITONAL INFO**
- Online Presence
- Information Sensibility
- Regulations
- Previous incidents

**3. CYBER RESULT**
- Breakdown of different loss categories;
- No. of of potential attackers;
- Probability by type of attack.

**4.INTRODUCE CYBERSHIELD**
Suggest plan and modules according to client profile. Ideally, store data for follow-up of the purchase.

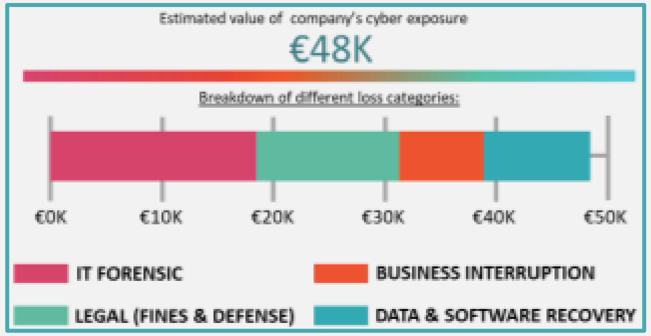



Figure 38: Preview of Ageas' Risk Assessment Tool

### Engaging Interactive Webinars

Figure 39: Webinar Agenda


**Actions: (1)** various **speakers** and a **host** to connect session moments; **(2)** several **pools** and **Q&As** during the webinar; **(3)** **game dynamics** – e.g. from the 3 emails which do you think is a phishing scam?

### Empowering salesforce

**Actions: (1)** Develop a **video demo** and provide this and other **learning resources** to brokers and agents; **(2)** **Attractive** sales **commissions**; **(3)** **Career opportunities**: best sellers gain the opportunity of taking a cyber insurance course to be certified as a specialized broker/agent.


Figure 40: Multimedia Demo of CyberShield

## Impact Measure KPIs

- Conversion Rates
- Written Premiums
- Bind and Quote Rate
- New Polices per Agent
- Customer Life-time value

[1]Inspired on Best Practice: Hiscox Cyber Exposure Calculator ***Sources***: *Hiscox, Team-based, Caravela*

# The "go-to-market" plan is underpinned in the omnichannel customer journey, which enables an excellent experience, not only to boost conversion rates but also to drive customer satisfaction and retention.

## F.5. Recommendations B2C | Develop an efficient "go-to-market" plan (I/III)

### VALUE CREATION

To customers: The marketing efforts demystify the complexity of the value proposition; in particular, the risk assessment tools allow individuals to confirm their cyber exposure and potential risks. To Ageas: The delivery of an omnichannel customer experience will boost marketing reach: the raise of awareness and engagement will be translated into higher conversion rates.

### DESCRIPTION

Map the **customer journey** as a guide to an efficient "go-to-market" plan.

- Place**:** Propose (by ranking) the most appropriate **Ageas' brands** to commercialize CyberShield; select **distribution channels** according to clients' preferences and insurance characteristics.
- Promotion**:** Develop **awareness and engagement strategies** to communicate the real value of the product.
- People**:** Facilitate **learning materials** and organize an **incentive program** to salesforce – brokers and agents (including remuneration and training)[1].
- Physical Evidence: In this industry, as the service is only experienced after the delivery, insurers help potential customers to perceive the value of the policy purchased by providing **testimonials**.

### RATIONALE

**Omnichannel Customer Experience Journey:** same reasoning applied as the B2B

- **Ageas' customer-centricity:** *"We exist for our customers."*

**Customer journey mapping** provides a common vision to all departments involved in the delivery of a superior customer experience. Thus, it guides a customer-centric go-to-market plan.

[1] Already developed in the B2B "go-to-market" recommendation.

***Sources:*** *Ageas Portugal,*

# Research reveals the prominence of digital and thus, Ocidental and Seguro Directo are the most appropriate brands. Ageas should leverage Norton's partnership to advertise CyberShield through its website and technology stores.

## F.5. Recommendations B2C | Develop an efficient "go-to-market" plan (II/III)

Further Detail: Appendix 31

### RATIONALE (continuation)

#### Qualitative Assessment of Ageas' Brands to commercialize CyberShield

| Ageas' Brands | ageas seguros | OCIDENTAL SEGUROS | SEGURO DIRECTO grupo ageas |
|---|---|---|---|
| 👍 | • Large client base<br>• Add-on to home insurance | • Large client base<br>• Add-on to home credit insurance<br>• Strong digital presence | • Strong customer experience<br>• Strong digital presence<br>• Possibility to leverage portfolio |
| 👎 | • Lack of digital presence | • Benchmarking evidence | • Misfit with the brand image |

*Table 32: Ageas brand's pros and cons to sell CyberShield*

#### Research Findings: Social Media Advertising

According to a PwC study:

- **90%** of consumers trust peer recommendations in social media;
- **79%** are more likely to recommend brands since becoming a follower;
- **71%** are more likely to purchase based on social media referrals.

#### Customer distribution channels preferences

- **Survey Insights:** Online (**36%**), physical stores (**33%**), agent (**17%**), mobile (**14%**)

#### Awareness and Engagement

- **Survey Insights:** Reasons for not having insurance: **lack** of **knowledge** (78%), **lack** of **necessity** (21%). The decrease in parents' WTP after the awareness video shows that resources must be moderated (appendix 13).

### RECOMMENDATION

| Recommended Brands[1]: | Insurance Structure: |
|---|---|
| 1 OCIDENTAL SEGUROS → | Add-on to Home Credit Insurance |
| 2 SEGURO DIRECTO grupo ageas → | Standalone Policy |
| 3 ageas seguros → | Add-on to Home Insurance |

**Distribution Channels:**

| | | |
|---|---|---|
| **Online** | Brands' Website & Social Media, E-mails, Homebanking, Norton's Website (appendix 31). | • Awareness<br>• Consideration<br>• Purchase |
| **Physical Stores** | Technology Stores (e.g. Worten, Fnac & MediaMarket) | • Consideration<br>• Purchase |

*Table 33: Distribution Channels*

[1]Most relevant factors: (1) Strong digital presence, (2) Possibility to offer add-on policy    ***Sources**: Ageas Portugal, PwC, Surveys*

# While the risk assessment tool enhances customer awareness, online marketing empowers CyberShield to become a more appealing product and Ageas to reach a larger audience and boost conversion rates.

## F.5. Recommendations B2C | Develop an efficient "go-to-market" plan (III/III)

Further Detail: Appendix 31

### RECOMMENDATION

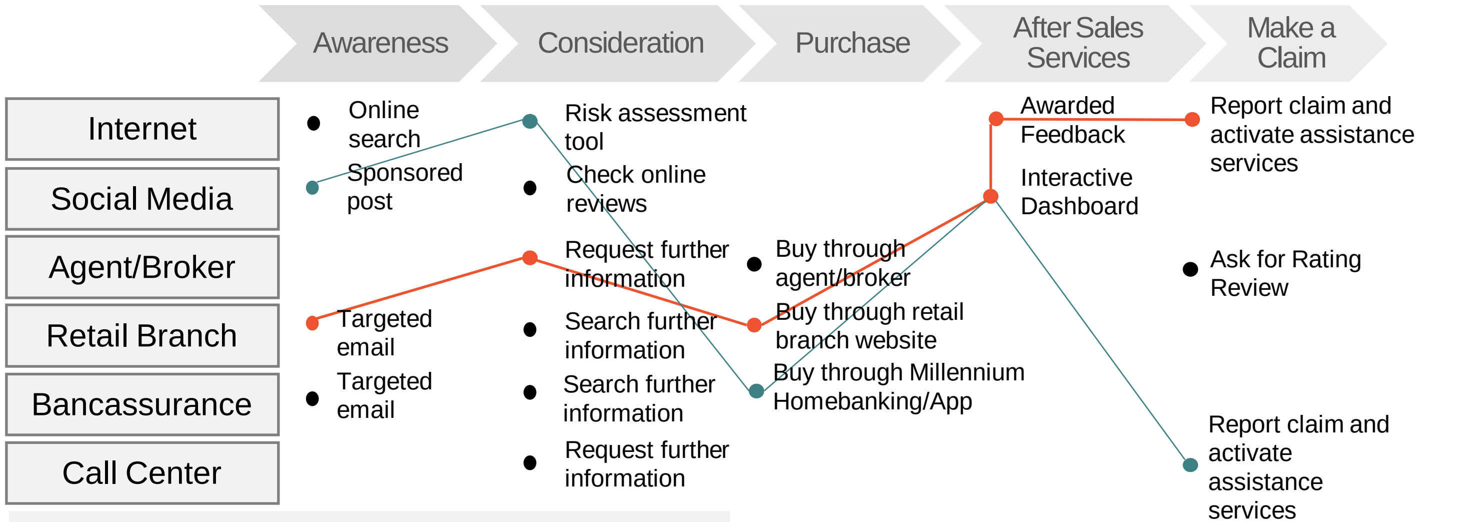



*Figure 41: Omnichannel Customer Journey*

### Risk Assessment Tool

| KEY DATA | | CYBER RESULT | | INTRODUCE CYBERSHIELD | |
|---|---|---|---|---|---|
| | **Checking for data breaches:**<br>• E-mail address<br>**Checking for identity theft:**<br>• E-mail address;<br>• Account password | | • Websites in which the e-mail has been compromised;<br>• Location and devices in which the account is logged in. | | Suggest plan and modules according to the client's profile. Ideally, store data for follow-up of the purchase (after approval). |

*Figure 42: Risk Assessment Tool (appendix 31 for illustration)*

### Social Media Strategy

| PARTNER | SELECTION REASONING |
|---|---|
| **Carolina Patrocínio**  | • Family-oriented;<br>• More than 929K followers;<br>• Top 15 influencers in Portugal;<br>• 2.70% engagement rate. |
| **Toni Vicente**  | • Tech-oriented;<br>• More than 39K YouTube subscribers;<br>• More than 870K accumulated views. |
| **Sara Barradas**  | • Previous victim of a cyber attack;<br>• More than 366K followers. |

*Figure 43: Potential Partners*

Ageas should develop **attractive social media posts** with **testimonials** from the suggested partners (appendix 31 for illustration). The content should be moderated – if people feel manipulated, the campaigns will have an adverse effect.

### Impact Measure KPIs

- Conversion Rates
- Policy Sales Growth
- Avg. Engagement Rate
- Referrals
- Customer Life-time Value

***Sources**: Norton, Ageas Portugal, "Have I Been Pwned?", Starngage*

# An efficient underwriting process entails a competitive edge, as it unlocks an insurer's ability to deliver comprehensive and bespoke solutions, at adequate pricing, while controlling the accumulation of losses.

## F.6. Recommendations B2B & B2C | Design solutions to overcome underwriting challenges (I/III)

Further Detail: Appendix 32

### VALUE CREATION

To customers: Standardization and transparency of coverages enable SMEs' comprehension and comparison of cyber insurances to perceive its actual value. To Ageas: An efficient underwriting process enables the delivery of comprehensive and tailored solutions at an adequate price while controlling claims and preventing the accumulation of losses.

### DESCRIPTION

Ageas should implement solutions to deal with underwriting challenges, namely the use of ISACs to collect data on aggregated loss or correlation scenarios, the adoption of a common taxonomy, the creation of effective feedback loops to enhance data gathering, and, to surpass tail risks, realistic disaster scenarios and risk transfer strategies, either through reinsurance or insurance-linked securities.

**Processes**

*"The actual procedures, mechanisms, and flow of activities by which the service is delivered – this service delivery and operating systems."*[1]

**Underwriting**

*"The process through which an individual or institution takes on financial risk for a fee"*[2]

### RATIONALE

Challenges in underwriting are related to the **evolving nature** and **recency** of cyber risk, which leads to a **shortage of available** and **standardized data.**

**Language Risks:** lack of standardization and transparency coverage policy due to the absence of an universal language.

- It challenges data collection on cyber incidents – as this implies the adoption of a common language – contributing to the lack of available and standardized data.

**Silent Cyber Risks:** situations in which cyber exposure is neither explicitly included nor excluded within an insurance policy. In 2019, only 5 out of 40 insurers stated that cyber risks were clearly excluded from their P&Cs[3] policies.

- Insurers may pay claims for unforeseen cyber losses not charged in premiums.
- A single event can trigger accumulation losses within other policies. E.g. 90% of $3B NotPetya losses were linked to silent cyber risks.

[1] Zeithaml & Bitner (2003), [2] Investopedia, [3]P&C – Property and Causality

***Sources**: ENISA, EIOPA, Deloitte*

# To overcome language and silent risks, Ageas should get involved with ISAC, adopt of a common taxonomy, establish a multi-department unit to review policies' exposures and provide clear coverage, exclusions and (sub)limits.

Further Detail: Appendix 32

## F.6. Recommendations B2B & B2C | Design solutions to overcome underwriting challenges (II/III)

### RATIONALE (continuation)

| | |
|---|---|
| **Modelling and Data Risks:** models and data have limited use in predicting the frequency and severity of events due to changing correlations. | • Leads to inadequate pricing, restricted coverage (with a lack of clarity on exclusions) and, ultimately, to customers doubting the value of the policies. |
| **Tail Risks:** unpredictable risk (low probability) that moves more than three standard deviations from the mean. (e.g. security failure in one of top cloud providers; cyber incident causing a blackout in a metropolitan area, etc.) | • Insurers may undertake more risk than their appetite; a single event can cause high losses, for multiple businesses and (re)insurers. (e.g. WannaCry is estimated to have caused financial and economic losses up to $4B.) |

### RECOMMENDATION

Ageas should **adopt** the proposed **strategic solutions** to surpass the previously identified underwriting challenges.

Solutions for Language Risks

| Support emerging initiatives aiming to collect data on aggregated loss or correlation scenarios | Contribute to language harmonization by adopting common terminology & taxonomy |
|---|---|
| • Explore data sharing, respecting customers' confidentiality, but providing sufficient data to support risk assessment;<br>• Use Information Sharing and Analysis Centres (ISACs): non-profit organisations allowing gathering and two-way sharing of information on cyber threats (e.g. ENCS[1]). | • Examples of commonly used taxonomies: ENISA, Lloyds or Chubb's COPE Framework (appendix 32);<br>• Ageas should follow the ENISA taxonomy, which divides post-breach services into three parts: 1st Party; 3rd Party and Other Benefits. |

*Table 34: Solutions for Language Risks*

Solutions for Silent Cyber Risks

| Develop strategies to identify silent risks in policies | Adopt clear policy language |
|---|---|
| • Example: Form a multi-department unit with members of the underwriting, claims and legal teams to measure individual and aggregate exposures. | • Ageas should offer policies with flexible coverage, that include appropriate and transparent requisites, exclusions, limits and sub-limits. |

*Table 35: Solutions for Silent Cyber Risks*

[1] European Network for Cybersecurity

***Sources:*** *Reinsurance News, ENISA, EIOPA, Deloitte*

# To surpass modelling and tail risks, Ageas should adapt risk management models, create effective feedback loops, implement realistic disaster scenarios and risk transfer strategies – reinsurance or insurance linked securities.

## F.6. Recommendations B2B & B2C | Design solutions to overcome underwriting challenges (III/III)

Further Detail: Appendix 32

### RECOMMENDATION (continuation)

| Solutions for Modelling and Data Risks |
|---|
| Adapt Model Risk Management (MRM) frameworks to cyber risk |
| • Shorter model validation cycles: frequent reviews of processes and disciplines focused on qualitative assessment (versus compliance);<br>• Develop systematic processes for the automated collection and treatment of claims Management Information (MI) – ensures back-testing accuracy and consequent improvement of MRM. |
| Create Effective Feedbacks Loops |
| • Architect systems to empower cross business lines and functions collaboration enabling frequent and quick flows of MI;<br>• Example: after linking claims to cyber events, the claims' team needs to immediately share the occurrence with the underwriting team, to investigate and update the MRM. |

*Table 36: Solutions for Modelling and Data Risks*

| Solutions for Tail Risks |
|---|
| Realistic Disaster Scenarios (RDS) |
| • Perform RDS (e.g. reverse stress test scenarios) to test extreme risks (high losses due to rare events) and potential accumulated risks (aggregate losses due to exposure correlations);<br>• Estimate the low probability scenarios that are most likely to harmfully impact businesses and assess the effect of potential aggregate losses arising from the scenario in question. |
| Reinsurance |
| • Ensure that the current agreement (Gen Re) reflects cyber exposures and that the wording is understood and robust, with the regular revision of risk transfer strategies;<br>• Quota Share Treaty (proportional premium and losses sharing based on a fixed percentage): maximum retention of 20% for Ageas and 80% ceded. |
| Insurance-Linked Securities (ILSs) |
| • ILSs are a specific type of reinsurance linked to pre-specified events (e.g. CAT bonds), provided by capital market investors;<br>• Allow insurers to offset risk and raise capital through risk diversification (away from general reinsurance) with a fully secure and collateralized form of funding. |

*Table 37: Solutions for Tail Risks*

### IMPACT MEASURE KPIs

- Claims Frequency
- Avg. Cost per Claim
- Claims Ratio
- Policy Sales Growth
- Bind Rate
- Customer Satisfaction

***Sources**: ENISA, EIOPA, Deloitte, Ageas Portugal*

# References (I/XII)


- Abbosh, Omar, and Bissel Kelly. 2019. “Securing the Digital Economy.” Accenture. 2019. https://www.accenture.com/us-en/insights/cybersecurity/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf#zoom=50. Accessed October 10.
- Aguilar, Francis J. 1967. Scanning the Business Environment. Macmillan.
- AJSEG. 2020. “AJSEG - Mediação de Seguros.” 2020. https://www.ajseg.pt/. Accessed September 30.
- Allianz. 2020. “Cyber Risks.” 2020. https://www.scal.pt/wp-content/uploads/2020/02/Allianz-Cyber-Risks-CP.pdf. Accessed September 28.
- Amadeo, Kimberly. 2020. “Brexit Consequences for the U.K., the EU, and the United States.” The Balance. 2020. https://www.thebalance.com/brexit-consequences-4062999. Accessed September 22.
- American International Group (AIG). 2020. “CyberEdge.” 2020. https://www.aig.com.pt/content/dam/aig/emea/portugal/documents/brexit/empresas/financiallines/cyberedge.pdf. Accessed September 10.
- Aníbal, Sérgio. 2020. “Taxas de Juro Da Dívida Portuguesa a Dez Anos Aproximam-Se de Zero.” Público, November 25, 2020. https://www.publico.pt/2020/11/25/economia/noticia/taxas-juro-divida-portuguesa-10-anos-aproximamse-zero-1940617. Acessed December 10.
- AON. 2019. “US Cyber Market Update.” http://thoughtleadership.aon.com/Documents/201906-us-cyber-market-update.pdf.
- Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF). 2020. “Prémios - Ranking Das Entidades (Mercado): Atividade Em Portugal e Estrangeiro (2015-2019).” 2020. https://www.asf.com.pt/NR/exeres/A6E856FF-AD45-40DD-83C7-8614A910D835.htm
- Banco de Portugal. 2020. “Boletim Económico.” https://www.bportugal.pt/sites/default/files/anexos/pdf-boletim/be_dez2020_p.pdf. Accessed December 20.

# References (II/XII)


- Banton, Caroline. 2020. “Underwriting.” Investopedia. 2020. https://www.investopedia.com/terms/u/underwriting.asp. Accessed October 14.
- Barney, Jay. 1991. “Firm Resources and Sustained Competitive Advantage.” Journal of Management. https://doi.org/10.1177/014920639101700108.
- BBVA Spain. 2020. “BBVA Spain.” 2020. https://www.bbva.com/es/. Accessed December 14.
- Bernard, Julie. 2020. “Overcoming Challenges to Cyber Insurance Growth.” https://www2.deloitte.com/us/en/insights/industry/financial-services/cyber-insurance-market-growth.html.
- Bissell, Kelly, and Larry Ponemon. 2019. “The Cost of Cybercrime.” https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.
- Booms, Bernard H., and Mary J. Bitner. 1981. “Marketing Strategies and Organization Structures for Service Firms.” Marketing of Services.
- Buehler, Kevin, Venky Anant, Tucker Bailey, James Kaplan, Mahir Nayfeh, and Wolf Richter. 2020. “Cybersecurity in a Digital Era.” McKinsey. 2020. https://www.mckinsey.com/~/media/McKinsey/Business Functions/Risk/Our Insights/Cybersecurity in a digital era/Cybersecurity in a Digital Era.pdf.
- Caravela Companhia de Seguros. 2020. “Cyber Risks.” 2020. https://www.caravelaseguros.pt/wp-content/uploads/2019/10/CYBER-RISKS-CG-CE.pdf. Accessed September 25.
- Catlin, Tanguy, Ewan Duncan, Harald Fanderl, and Johannes-Tobias Lorenz. 2016. “The Growth Engine: Superior Customer Experience in Insurance.” https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/the%20growth%20engine%20superior%20customer%20experience%20in%20insurance/the_growth_engine_superior_customer_experience_in_insurance_may_2016.ashx

# References (III/XII)


- Centro Nacional de Cibersegurança (CNCS). 2019a. "Quadro Nacional de Referência Para a Cibersegurança." https://www.cncs.gov.pt/content/files/cncs_qnrcs_2019.pdf.
- ———. 2019b. "Relatório Cibersegurança Em Portugal - Sociedade." https://www.cncs.gov.pt/content/files/relatrio_sociedade_2019_-_observatrio_de_ciberseguranca_cncs_v3.pdf.
- ———. 2020. "Relatório Cibersegurança Em Portugal - Riscos e Conflitos." https://www.cncs.gov.pt/content/files/relatorio_etica.direito2020__observatoriociberseguranca_cncs.pdf.
- Christopher, M. 1992. Logistics & Supply Chain Management: Creating Value-Adding Networks.
- Chubb Portugal. 2020. "Cyber Enterprise Risk Management." 2020. https://www.chubb.com/pt-pt/products/cyber-enterprise-risk-management.html.
- Cohen, Russ. 2016. "Cyber COPE® Transforming Cyber Underwriting." https://www.chubb.com/content/dam/chubb-sites/chubb-com/us-en/business-insurance/transforming-cyber-underwriting/documents/pdf/chubb-cyber-cope-whitepaper_09.16.pdf.
- Crozdesk. 2017. "OutThink Pricing." 2017. https://crozdesk.com/it/cyber-data-security/outthink/pricing. Accessed December 13.
- D'Alessandro, Paul, Dean Nicolacakis, Tom Puthiyamadam, and Karen Wilson. 2014. "Embracing the 'Always on' Customer." https://www.pwc.com/cl/es/publicaciones/assets/embracing-the-always-on-customer.pdf.
- Data Privacy Manager. 2019. "GDPR Fines." Data Privacy Manager. 2019. https://dataprivacymanager.net/glossary/gdpr-fines/. Accessed October 28.
- Deloitte Cyprus. 2017. "Cyber Insurance - A Key Element of the Corporate Risk Management Strategy." https://www2.deloitte.com/cy/en/pages/risk/articles/cyber-insurance.html.

# References (IV/XII)


- Diário da República. 2009. Código Do Trabalho - Lei n.o 7/2009. República Portuguesa. https://dre.pt/legislacao-consolidada/-/lc/75194475/201608230300/73439892/diploma/indice.
- Douligeris, Christos, Omid Raghimi, Barros Lourenço, and Marco. 2020. “Threat Landscape 2020 - Phishing.” https://www.enisa.europa.eu/publications/phishing.
- ECO Seguros. 2020. “Ranking: As Maiores Seguradoras de Portugal Em 2019,” February 4, 2020. https://eco.sapo.pt/2020/02/04/contas-finais-producao-de-seguros-caiu-51-em-2019/.
- Enterprise Ireland. 2019. “The European Cybersecurity Market - Mapping the Opportunities and Route to Market for Irish SMEs.” https://globalambition.ie/wp-content/uploads/2019/11/The-European-Cybersecurity-Opportunities-for-Irish-SMEs_Key-Takeouts.pdf.
- Entrust Solutions. 2020. “Artificial Intelligence and Cyber Crime: Facing New Threats.” 2020. https://www.entrustsolutions.com/wp-content/uploads/2020/07/NKQUIPo-scaled.jpg.
- European Commission. 2015. “Special Eurobarometer 423 - Cyber Security.” https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf.
- ———. 2020. “The EU Cybersecurity Act.” 2020. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.
- European Network of Cyber Security (ENCS). 2020. “ENCS.” 2020. https://encs.eu/. Accessed 12 November.
- European Union. 2018. “What Is GDPR, the EU’s New Data Protection Law?” 2018. https://gdpr.eu/what-is-gdpr/.
- European Union Agency for Cybersecurity (ENISA). 2017. “Commonality of Risk Assessment Language in Cyber Insurance.” https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance.

# References (V/XII)


- ———. 2018. “NIS Directive.” European Network and Information Security Agency. 2018. https://www.enisa.europa.eu/topics/nis-directive.
- Eurostat. 2019. “Enterprises Having Insurance against ICT Security Incidents.” 2019. https://appsso.eurostat.ec.europa.eu/nui/show.do?query=BOOKMARK_DS-132947_QID_5B6DBB83_UID_-3F171EB0&layout=SIZEN_R2,L,X,0;GEO,L,Y,0;INDIC_IS,L,Z,0;TIME,C,Z,1;UNIT,L,Z,2;INDICATORS,C,Z,3;&zSelection=DS-132947INDIC_IS,E_SECINS;DS-132947UNIT,PC_ENT;DS-13294
- ———. 2020. “Wages and Labour Costs.” Eurostat Statistics Explained. 2020. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Wages_and_labour_costs.
- FERMA. 2018. “Preparing for Cyber Insurance.” https://www.ferma.eu/app/uploads/2019/02/preparing-for-cyber-insurance-web-04-10-2018.pdf.
- Fidelidade. 2020a. “Cyber Famílias.” 2020. https://www.fidelidade.pt/PT/particulares/Familia/Seguros/cyber-familias/Documents/Cyber Familias_JI001_CG001_out2020.pdf. Accessed 24 November.
- ———. 2020b. “Cyber Safety.” 2020. https://www.fidelidade.pt/PT/empresas/cs/Documents/RC009_CG196–Seguro_Responsabilidade_Civil–Cyber_Safety_Out2020.V1.pdf. Accessed 13 September.
- Financial Stability Board. 2018. “Cyber Lexicon.” https://www.fsb.org/wp-content/uploads/P121118-1.pdf.
- Friedman, Sam, and Adam Thomas. 2017. “Demystifying Cyber Insurance Coverage.” https://www2.deloitte.com/us/en/insights/industry/financial-services/demystifying-cybersecurity-insurance.html.
- Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU). 2016. “One in Two Users Click on Links from Unknown Senders.” 2016. https://www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders/.

# References (VI/XII)


- Gard, Jean-Christophe, and Ofir Eyal. 2012. "The Six Steps to Pricing Power in Insurance." https://www.bcg.com/publications/2012/six-steps-to-pricing-power-insurance.
- Garg, Ashu, and Siddhant Trivedi. 2019. "Cybersecurity: The Next Trillion-Dollar Market?" Foundation Capital. 2019. https://foundationcapital.com/cybersecurity-the-next-trillion-dollar-market/.
- Grundy, Tony. 2006. "Rethinking and Reinventing Michael Porter's Five Forces Model." Strategic Change. https://doi.org/10.1002/jsc.764.
- Grupo Ageas Portugal. 2020. "Grupo Ageas Portugal." 2020. https://www.grupoageas.pt/. Accessed 3 September.
- Gupta, Sunil. 2014. "Core Curriculum: Segmentation and Targeting." Harvard Business School.
- Gupta, Sunil, and Jill Avery. 2014. "Core Curriculum: Brand Positioning." Harvard Business School.
- Hay, Laura J., Frank Ellenburger, Christian Schareck, and Claudia Fell. 2020. "New Reality for Insurance: Germany." https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/09/new-reality-for-insurance-germany-insurance-value-chain-commercial-insurance.pdf.
- Hiscox. 2018. "2018 HISCOX Small Business Cyber Risk Report TM." https://www.hiscox.com/documents/2018-Hiscox-Small-Business-Cyber-Risk-Report.pdf.
- ———. 2019. "Hiscox CyberReadiness Report 2019." https://www.hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report_2019.PDF.
- Humphrey, Albert S. 2005. "SWOT Analysis for Management Consulting." SRI Alumni Association Newsletter.
- IBM. 2015. "IBM Security Services 2014 Cyber Security Intelligence Index for Financial Services." https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF.
- Innovarisk Underwriting. 2020. "CyberClear: Seguro de Riscos Cibernéticos." 2020. https://innovarisk.pt/wp-content/uploads/2018/05/CEspeciais_CyberClear.pdf.

# References (VII/XII)


- Instituto Nacional de Estatística (INE). 2020. "Sociedade Da Informação e Do Conhecimento - Inquérito à Utilização de Tecnologias Da Informação e Da Comunicação Nas Famílias." November 2020. https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=415621509&DESTAQUESmodo=2&xlang=pt.
- Insurance Europe. 2018. "Examples of Cyber-Resilience Initiatives by National Insurance Associations." https://www.insuranceeurope.eu/sites/default/files/attachments/National examples A5.pdf.
- Insurance Journal. 2019. "State of the Cyber Insurance Market- Top Trends, Insurers and Challenges: A.M. Best." Insurance Journal. https://www.insurancejournal.com/news/national/2019/06/18/529747.htm.
- International Communication Union (ITU). 2018. "Global Cybersecurity Index (GCI) 2018." https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.
- International Organization for Standardization (ISO). 2018. "International Organization for Standardization (ISO) - Online Browsing Platform." ISO/IEC 27000:2018(En): Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary. 2018. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en.
- Kaspersky. 2020. "5G and Cyber Security - All You Need to Know." Kaspersky. 2020. https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons.
- Kerin, Roger A. and Peterson, Roger A. 2010. Strategic Marketing Problems: Cases and Comments. 12th ed. Pearson Prentice Hall.
- Kotler, Philip, and Kevin Keller. 2005. Marketing Management. 12th ed. Pearson Prentice Hall.
- Kotler, Philip, Veronica Wong, John Saunders, and Gray Armstrong. 1996. Principles of Marketing. www.pearsoned.co.uk/.

# References (VIII/XII)


- KPMG South Africa. 2018. “Cyber Insurance – How Insuretechs Can Unlock The Opportunity.” https://assets.kpmg/content/dam/kpmg/za/pdf/2017/12/17383MC-cyber-insurance.pdf.
- Malhotra, Naresh K, Dan Nunan, and David Birks. 2017. Marketing Research: An Applied Approach. 5th ed. Pearson. https://www.pearson.com/uk/educators/higher-education-educators/program/Malhotra-Marketing-Research-An-applied-approach-5th-Edition/PGM1638972.html?tab=formats.
- MarketLine. 2018. “Insurance in Portugal.” https://advantage-marketline-com.eu1.proxy.openathens.net/Analysis/ViewasPDF/portugal-insurance-70159.
- Markow, Will, Scott Bittle, and Pang-Cheng Liu. 2019. “The State of Cybersecurity Report 2019.” https://www.wipro.com/applications/form/the-state-of-cybersecurity-report-2019/?asd.
- Marsh Portugal. 2020. “Risco Cibernético.” 2020. https://www.marsh.com/pt/pt/services/cyber-risk.html. Accessed 20 September.
- MDS. 2020. “Cyber Risk.” 2020. https://www.mdsgroup.pt/pt/seguros/empresas/produtos/patrimonio/cyber-risk/. Accessed 22 September.
- Merrey, Paul, Matthew Smith, Matthew Martindale, and Arturs Kokins. 2017. “Seizing the Cyber Insurance Opportunity.” https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/07/cyber-insurance-report.pdf.
- Meuser, Michael, and Ulrike Nagel. 2009. “The Expert Interview and Changes in Knowledge Production.” In Interviewing Experts. https://doi.org/10.1057/9780230244276_2.
- Microsoft. 2020. “Microsoft Digital Defense Report.” https://www.microsoft.com/en-us/download/details.aspx?id=101738.
- Minto, Barbara. 2002. The Pyramid Principle: Logic in Writing and Thinking. 3rd ed. Financial Times Prentice Hall.

# References (IX/XII)


- North American Industry Classification System (NAICS) Institution. 2020. “NAICS Code List.” 2020. https://www.naics.com/search/. Accessed September 28.
- Norton. 2020. “NortonTM 360.” 2020. https://pt.norton.com/products/norton-360-deluxe.
- Ocidental. 2020. “Grupo Ageas Portugal - Ocidental.” 2020. https://www.ocidental.pt.
- Orbis. 2020. “List of Portuguese Companies.” 2020. https://orbis-bvdinfo-com.eu1.proxy.openathens.net/version-20201217/orbis/1/Companies/Search.
- Organisation for Economic Co-operation and Development (OECD). 2017. Enhancing the Role of Insurance in Cyber Risk Management. OECD Publishing. OECD. https://doi.org/10.1787/9789264282148-en.
- ———. 2018. “Unleashing the Potential of the Cyber Insurance Market - Conference Outcomes.” https://www.oecd.org/daf/fin/insurance/Unleashing-Potential-Cyber-Insurance-Market-Summary.pdf.
- ———. 2020a. “Country Statistical Profiles - Italy.” OECD Data. 2020. https://data.oecd.org/italy.htm.
- ———. 2020b. “Purchasing Power Parities (PPP).” OECD Data. 2020. https://data.oecd.org/conversion/purchasing-power-parities-ppp.htm.
- OutThink. 2020. “OutThink.” 2020. https://outthink.io/.
- PCI Security Standards Council. 2020. “PCI Security Standards Council.” 2020. https://www.pcisecuritystandards.org.
- Poletto, Yuri. 2019. “Quali Sviluppi per El Mercato Cyber.” Insurance Daily, January 16, 2019. https://www.insurancetrade.it/insurance/archivio/insurance-daily?page=46.

# References (X/XII)


- PORDATA. 2019. “Agregados Familiares Por Escalões de Rendimento: IRS Modelo 1+ 2.” 2019. https://www.pordata.pt/Portugal/Agregados+familiares+por+escalões+de+rendimento+IRS+Modelo+1++2-79.
- ———. 2020a. “Assinantes Do Acesso à Internet.” 2020. https://www.pordata.pt/Portugal/Assinantes+do+acesso+à+Internet-2093.
- ———. 2020b. “Indicadores de Envelhecimento.” 2020. https://www.pordata.pt/Portugal/Indicadores+de+envelhecimento-526.
- ———. 2020c. “Taxa Real de Escolarização.” August 2020. https://www.pordata.pt/Portugal/Taxa+real+de+escolarização-987.
- Porter, Michael E. 1985. “Competitive Advantage.” The Free Press.
- ———. 1979. “Competitive Forces Shape Strategy.” Harvard Business Review.
- ———. 1980. Competitive Strategy: Techniques for Analyzing Industries and Companies. New York.
- Reinsurance News. 2017. “Total WannaCry Losses Pegged at $4 Billion.” 2017. https://www.reinsurancene.ws/total-wannacry-losses-pegged-4-billion/.
- Rennie, David. 2020. “The Biden Administration Will Try to Box Clever on China.” The Economist. https://www.economist.com/the-world-ahead/2020/11/16/the-biden-administration-will-try-to-box-clever-on-china.
- Seguro Direto. 2020. “Seguro Directo.” 2020. https://www.segurodirecto.pt.
- Seguros 24. 2020. “Seguro Cyber Risks.” 2020. https://www.seguros24.pt/empresas/cyber-risks/.
- Septor. 2020. “Seguro Riscos Cibernéticos.” 2020. https://septor.pt/protocolos/cyber-risks/.

# References (XI/XII)


- Standage, Tom. 2020. "Ten Trends to Watch in the Coming Year." The Economist. https://www.economist.com/the-world-ahead/2020/11/16/ten-trends-to-watch-in-the-coming-year.
- Starngage. 2020. "Top 1000 Influencers in Portugal." 2020. https://starngage.cn/ph/influencer/ranking/portugal?page=1.
- Statista. 2020. "Number of Internet Users Worldwide from 2005 to 2019." 2020. https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/.
- The World Bank. 2020. "Individuals Using the Internet (% of Population)." 2020. https://data.worldbank.org/indicator/IT.NET.USER.ZS.
- Thoms, Glyn. 2020. "Cyber Claims Analysis Report." https://www.willistowerswatson.com/en-AU/Insights/2020/07/cyber-claims-analysis-report.
- Touchstone Security. 2020. "5 Benefits of Security Awareness Training." 2020. https://touchstonesecurity.com/security-training/.
- Tranquilidade. 2020a. "Seguro Cyber Risks." 2020. https://www.tranquilidade.pt/documents/5723202/5739832/Mod.+732.081+-+mar+2018+-+CG+Cyber+Risks.pdf/5374fb1d-2da0-4354-9652-1017c37962b2.
- ———. 2020b. "Tranquilidade Seguro Multirrisco Empresarial." October 2020. https://www.tranquilidade.pt/documents/5723202/5739832/Mod.+337.031+-+mar+2018+-+CG+MR+Empresarial.pdf/58a37cdc-c942-4606-bfa7-a14349e6f244.
- United Nations Conference on Trade and Development. 2020. "Data Protection and Privacy Legislation Worldwide." 2020. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.
- Verizon. 2020. "Data Breach Investigations Report." https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.
- Vernon, Raymond. 1966. "International Investment and International Trade in the Product Cycle." Quarterly Journal of Economics. https://doi.org/10.2307/1880689.

# References (XII/XII)


- Visavis. 2020. “Cyber Risks.” 2020. https://www.visavis.pt/index.php?module=home&func=areas#cyber.
- Ward, Robert. 2020. “The World Economy after the US Elections.” International Institute for Strategic Studies. 2020. https://www.iiss.org/events/2020/10/prospects-for-the-global-economy-us-election-and-covid19.
- Warren Lynch. 2020. “Strategic Planning to Actionable Items: From SWOT to TOWS Analysis.” 2020. https://warren2lynch.medium.com/from-swot-to-tows-analysis-55ac394064b7.
- Willi, Fabian, and Maya Bundt. 2019. “Personal Cyber Insurance: Protecting Our Digital Lives.” https://www.swissre.com/dam/jcr:68e4d8fb-509c-4182-a219-c803f7d23af1/ZRH-18-00632-P1_Personal_cyber_insurance_Publication_WEB.pdf.
- World Economic Forum. 2020. “Regional Risks for Doing Business.” https://widgets.weforum.org/regionalrisks2020/.
- Zeithaml, V.A., and M.J. Bitner. 2003. Services Marketing Integrating Customer Focus across the Firm. 3rd ed. New York.: Irwin McGraw-Hill,.

## Agenda

## Team Members

### AFONSO GOMES

- BSc in Economics at Nova School of Business and Economics
- International MSc in Management at Nova SBE – Specialization in Strategy and International Business
- Industry experience in Banking

### MADALENA SANGALHO

- BSc in Management Nova School of Business and Economics
- International MSc in Management at Nova SBE – Specialization in Strategy and International Business
- Industry experience in Aircraft Ground Handling

### RAQUEL BRITES

- BSc in Management at Nova School of Business and Economics
- MSc in Management at Nova SBE – Specialization in Strategy and International Business
- Co-President at *Nova Women in Business*

***Sources**: Team-based*

# APPENDIX 1 – PROJECT TEAM

## Belbin Analysis

| TEAM MEMBER | PRE President | STR Strategist | INT Intellectual | MON Monitor | OPE Operational | TW Team Worker | PRO Prospector | FIN Finisher |
|---|---|---|---|---|---|---|---|---|
| Afonso Gomes | | | | | ☑ | ☑ | | |
| Madalena Sangalho | | ☑ | | | | | | ☑ |
| Raquel Brites | ☑ | | | ☑ | | | | |

### Implications For The Team

In a preliminary phase, the team conducted a best practice for team building and performance optimization – Belbin Analysis. The assessment of relative behavioral strengths and weaknesses in the workplace disclosed the most suitable team roles for each member and provided a common language for efficient communication. The team realized the absence of a member with the **Intellectual** – delivers scarce and detailed information on request – and **Prospector** – explores external information sources. To mitigate the lack of these roles, the team conducted eleven **industry experts' interviews** and attended a "**Design Thinking**" course to implement effective brainstorming techniques and tools (e.g., Miro App). Nevertheless, it is important to highlight the team's strong points resulting from the President and Team Worker roles. The active listening and co-operation empowered the team to leverage client syndication and to surpass numerous obstacles. Hence, the team was able to maintain the focus on delivering a superior solution.

***Sources**: Team-based*

## Individual Reflections (I/III)

### AFONSO GOMES

**Team Worker**

**Operational**

**Intellectual**

**Finisher**

**<u>Team Worker</u>**: leverages on its cooperation and diplomatic skills to effectively listening and building.

**<u>Operational</u>**: implements the teams' work with an efficient organisational frame.

### Tetramap Elements

**<u>Fire</u>**: *"Like the sun is bright"*

The fire element relies on its positivity to explore possibilities and influence others to also look at the positive side of life. Their great sense of fun and love for variety distinguishes them in a team.

**<u>Water</u>**: *"Like a lake is calm"*

The water element is caring and consistent and crucial to hold teams together. They aspire to work in an environment with harmony and flow and show a high level of effort and patience.

### Key Learnings

The Consulting lab allowed me to have a first real consulting experience and reinforced my aspiration to start my professional career in this industry. Developing the cyber risk challenge with Ageas allowed me to gain real knowledge in the insurance industry, and in particular in such a complex and unknown topic as cyber risk.

Moreover, I believe that the key success factor of this project was communication, both inside the team and with the client. The frequent feedback and conjunction of different ideas and perspectives with my colleagues were crucial to reach higher outcomes and develop efficient solutions.

Finally, continuous syndication with the client allowed for the management of expectations and making sure the team was on the right track. Besides this, the acknowledgment and possible implementation of our outputs by the client is a truly rewarding feeling.

***Sources**: Belbin Model, Tetramap Model, Team-based*

## Individual Reflections (II/III)

### MADALENA SANGALHO

Finisher

Strategist

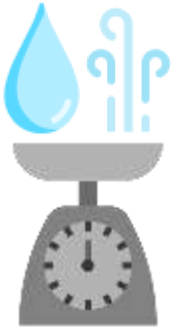
Monitor

Intellectual

**Finisher**: able to conscientiously find error and omissions to achieve a flawless delivery.

**Strategist:** studies and maps the future, by analysing patterns and trends.

### Tetramap Elements



**Water**: *"Like a lake is calm"*

The water element is caring and consistent and crucial to hold teams together. They aspire working in an environment with harmony and flow and show a high level of effort and patience.

**Air**: *"Like the wind is clear"*

The air element is highly analytical, relying on order and focus. They assure accuracy and quality in their work, by finding logical solutions to the faced challenges.

### Key Learnings

The Consulting Lab with Ageas Portugal granted me unparallel learning experiences, at a personal and professional level. Besides the enhancement of technical (analytical and problem-solving) capabilities, the client and team dynamics allowed me to enrich my interpersonal skills.

Throughout these four months, I was able to grasp the prominence of continuous syndication to build a trusting relationship with the client, which highly contributed to the success of the project. Furthermore, through companionship, the team transformed complex challenges into exciting self-growth opportunities. Therefore, by addressing a topic distant from my academic field, I was able to foster my adaptability, resilience, and creativity skills.

Finally, this real-life project assured me that consultancy perfectly fits my profile and career aspirations. It is dynamic, challenging, and allows me to explore diverse industries and competencies to grow into a complete and versatile professional.

**Sources**: *Belbin Model, Tetramap Model, Team-based*

# APPENDIX 1 – PROJECT TEAM

## Individual Reflections (III/III)

### RAQUEL BRITES

**President**

**Monitor**

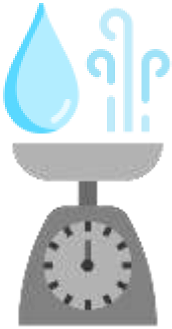
**Strategist**

**Finisher**

**President**: focuses on efficiently delegating tasks, clarifying goals and promoting decision-making.

**Monitor:** able to see all options and accurately judge them.

### Tetramap Elements



**Water**: *"Like a lake is calm"*

The water element is caring and consistent and crucial to hold teams together. They aspire working in an environment with harmony and flow and show a high level of effort and patience.

**Air**: *"Like the wind is clear"*

The air element is highly analytical, relying on order and focus. They assure accuracy and quality in their work, by finding logical solutions to the faced challenges.

### Key Learnings

The development of the Cyber Risk Challenge with Ageas Portugal, within the scope of the Consulting Lab, allowed me to convert my theoretical academic knowledge, from the last four years, into actions.

The major key learnings were related to the understanding of how a real-life project in Consulting works and, specifically, how the client-advisor bond begins and evolves towards a trusted relationship, crucial to a successful outcome. This ongoing syndication has also enabled me to learn with the clients' expertise and get practical experience in an unknown field – insurance.

Finally, working every day, for the past four months, with my colleagues towards a common goal has allowed me to not only develop my team-working skills but also to learn new methods and approaches to conduct analyses and formulate strategic options.

***Sources**: Belbin Model, Tetramap Model, Team-based*

## Agenda

## Political

- **Covid-19 Pandemics** causing political changes worldwide, with the imposition of temporary and total or partial lockdowns in many countries;
- **Political instability** leading to higher geopolitical risks – in which cyber is included:
  - **Brexit** leading to economic and political changes, with growing anti-EU parties in countries such as France and Germany threatening the union's stability;
  - Recent outcome in the **US elections** may ease tensions in trade (particularly with China) – trade barriers expected to be gradually dismantled.
- In Portugal, cyber is the primary risk for enterprises. Government has already implemented measures that aim to increase national resilience:
  - Creation of *Centro Nacional de Cibersegurança* in 2014, with the objective of preventing, detecting, and reacting to cyber incidents to State bodies and operators of essential services and digital service providers. – has helped raise awareness in Portugal to cyber risk and is contributing to an increase in cybersecurity skilled workers.

## Economic

**Covid-19 Pandemics** economic impact**:** the emergence of a vaccine in 2021 represents a sign of recovery for the world economy, after a year of recession. In Portugal, in 2021 is expected:

- **Economic Recovery:** GDP expected to decline 9.5% in 2020, recovering 5.2% in 2021;
- **Unemployment** will peak in 2021 and remain above pre-crisis level until 2022;
- **Private consumption** is expected to start recovering in 2021, after a 6,8% decrease in 2020. It is expected that by the end of 2022, it reaches pre-pandemic crisis levels;
- **Interest rates** on public debt at historically low levels (0,025%), as a result of monetary stimulus measures from the ECB to deal with the pandemic situation.

***Sources**: The Balance, Banco de Portugal, Economic Forum, INE, The Economist*

## Social

**Covid-19 pandemics** social impact:

- **Change in consumer behavior** - sharp rise in online shopping - in Portugal, the percentage of e-commerce users registered the highest increase since 2002, with a 7% rise compared to 2019;
- **Shift to remote** work has led to an increase in cybercrime – contributed to raising awareness among companies and individuals. - CNCS registered a 76% increase in the number of incidents registered in the month of March 2020, compared to the same period in 2019.

**Portuguese population:**

- Aging population – aging index increased from 121,6 to 161,34 from 2010 to 2018 (elderly per 100 youths)
- Medium-low-income levels compared to the median of Europe (84% of European average wage)
- Growing literacy levels: the % of enrolled students in high school in Portugal went from 71,4% in 2010 to 81,5% in 2019.

***Sources**: INE, CNCS, Pordata*

# APPENDIX 2 – PESTL (III/III)

Back to Presentation

## Technological

- **Cloud-based services & 5G** expanding cyber-attacks' opportunities along the entire supply chain:
  - To being with, 5g networks have a higher number of traffic routing points, that must be monitored in order to guarantee complete safety. Besides this, the increase in the speed and volume of data may challenge current monitoring methods. In addition, there is an increasing number of connected devices (smart TVs, refrigerators, etc.) that lack effective security and constitute new potential entry points for attackers.
- **Artificial Intelligence** automates the cyber-criminal process, allowing for increasingly sophisticated and targeted large-scale cyber attacks. Examples of these attacks are hacking of surveillance technologies, manipulation of algorithms (that can destroy a company's information systems, bypassing of physical recognition systems, AI to imitate the human voice, etc.)
- **Companies' digital innovation** is happening faster than their ability to secure it in 80% of cases.

## Legal

**Data protection and cybersecurity laws** are contributing to raising awareness to cyber risk among companies and individuals:

- **GDPR:** implemented in May 2018, consists of provisions on notifying and indemnifying data breaches. The main objective of this regulation is to increase individuals' control of personal data and simplify the regulatory environment for international business among the EU.
- **NIS Directive:** towards DSPs and OESs, aims at increasing cybersecurity across Europe. The directive consists of three parts: 1) **national capabilities** that countries in the EU must have in terms of cybersecurity (e.g., creation of a national cybersecurity center); 2) cross-border collaboration 3) national supervision of critical sectors (energy, transport, water, etc.) and critical digital service providers (online search engines, cloud, and marketplaces)
- PCI-DSS – information security standard for companies that commercialized online payments (credit, debit cards, etc.) to deal with card schemes.
- **EU Cybersecurity Act:** certification for digital products, services, and processes in the EU.

***Sources**: Kaspersky, Entrust Solutions, GDPR.EU, ENISA*

## Agenda

## Threat Of New Entrants

**High capital requirements** mainly in research and advertising expenditure – expertise and customer recognition are key elements in the insurance market;

**Distribution channels** are accessible but with tight profit margins, in traditional ones (agents, brokers, bancassurance, etc.). However, growth in e-commerce may ease the entry of new players due to lower costs;

**Financial services** companies starting to enter the insurance market – may see cyber insurance as a good market opportunity. Nevertheless, these companies are often constrained by regulation to sell insurance products;

**Government regulation:** high degree of legislation and compliance, both at a national level (by ASF) and at a European level (e.g., Solvency II directive) constitutes a considerable barrier to entry;

The threat of new entrants in the cyber insurance market is **medium**.

## Threat Of Substitutes

There exist **no real substitutes** for cyber insurance products. Cybersecurity providers offer pre-breach and post-breach services but do not cover for losses arising from cyber-attacks:

**Alternatives** to cyber insurance (and insurance products overall) include savings and investments but these options do not offer the same level of protection (coverage usually lower than in an insurance product);

**"Self-insurance"** is a risk management strategy in which a certain amount of money set aside to cover a specific risk. This alternative is ineffective and risky due to the unpredictability of the impact and frequency of cyber risks;

The threat of substitutes in the cyber insurance market is **low.**

## Bargaining Power Of Suppliers

Companies are usually dependent on **one supplier**, that usually has patented systems, originating an incentive for insurance companies to keep their suppliers, increasing their power;

**High degree of differentiation** of software companies – which provide tailored software to insurers' needs. – increases supply power;

**Backward integration** of software and ICT companies by cyber insurers is unlikely;

**Large-sized suppliers** (namely reinsurers such as Munich RE or Swiss Re) with high negotiating power;

The bargaining power of suppliers is **high.**

***Sources**: MarketLine, Team Based*

Back to Presentation

## Bargaining Power of Buyers

**Large number of customers** meaning that the impact of one customer on the insurer is minimal.

Customers are SME's (in the B2B segment) and individuals (in the B2C segment), with **low negotiating power** with insurers. Large companies have higher bargaining power but account for less than small/medium business in terms of premiums.

**Access to information is high**, as customers have access to multiple price-comparison websites, that allow choosing the best offer, leading to lower customer loyalty and high price sensitivity, which leads to a rise in buyer power.

In the future, in case insurance against third-party losses becomes a **legal obligation for companies**, this will decrease their bargaining power, as demand will become inelastic.

Switching costs for the consumer are high if customers plan to discontinue their policy after the cooling off period. When the term policy reaches the end, the customer can easily choose a different company for the next policy, meaning that overall **switching costs are medium**

**Product differentiation** is low in cyber insurance, with most competitors offering similar coverage. Companies are starting to differentiate in terms of pre-breach services, but customers decision is still mainly on price, meaning that they have increased power.

The bargaining power of buyers is **medium.**

## Competition Rivalry

The cyber insurance market in Portugal is dominated by Fidelidade, Allianz, and Tranquilidade, with other smaller insurers (Caravela, Innovarisk, AIG) in the market, contributing to a high level of rivalry.

The overall insurance market in Portugal is characterized by **a high concentration**, given that the four largest players have a concentration ratio of 67,5%. The four largest players are already in the cyber insurance market or preparing to enter it, and we can assume that they will have a similar concentration, given the large customer base and reputation of these insurers.

**Product differentiation** in this market can be considered as low, given that most players offer similar services and coverage, meaning that there is a high price sensitivity and low margins. Nevertheless, some players are starting to differentiate in pre-breach services.

This is an industry in a **growth stage**, with a rising number of competitors, meaning that rivalry is increasing.

**Entry barriers are high** given the legal requirements to enter the insurance market, namely capital adequacy, that prevents insurers from going out of business, to protect policyholders. This imposes **high barriers to exit**, such that big players, in case of economic turndown, will adopt aggressive strategies to retain clients and resist, increasing rivalry.

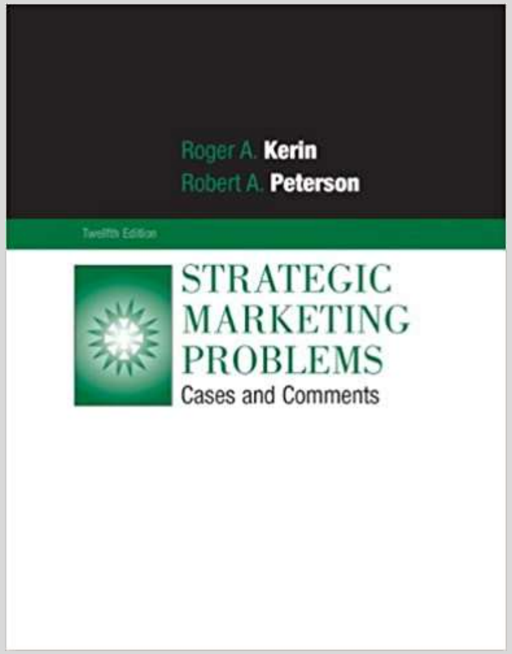
Competition rivalry in the Portuguese cyber insurance market is **high**.

***Sources***: *MarketLine, Team Based*

## Agenda

## Chain Ratio Method – Explanation

### Estimating Market Sales Potential [Chapter 4]




Three variables considered in estimating market sales potential:

1) *"The number of prospective buyers (B) who are willing and able to purchase an offering;"*
2) *"The quantity (Q) of an offering purchased by an average buyer in a specific period, typically one calendar year."*
3) *"The price (P) of an average unit of the offering;"*

$$Market\ sales\ potential = B \times Q \times P$$

*"This expression contains the building blocks for developing a more complex formulation through what is called **chain-ratio method**, which involves **multiplying a base number** by **several adjusting factors** that are believed to influence markets sales potential."*

### Method 1 – Chain-ratio Method

1 Forecast the **VOLUME**

**Total Available Market**

SMEs and families with the need & financial ability to buy cyber insurance

Willingness to buy or replace

**Serviceable Available Market**

SMEs and families with or willing to buy cyber insurance

Market Share

**Serviceable Obtainable Market**

Ageas reasonably expects to acquire.

*Chain Ratio Method to forecast market size*

2 Forecast the **PRICE**

## Methodology (Method 1)

1 Forecast the **VOLUME**

**Total Available Market**

SMEs and families with the need & financial ability to buy cyber insurance

Willingness to buy or replace

**Serviceable Available Market**

SMEs and families with or willing to buy for a cyber insurance

Market Share

**Serviceable Obtainable Market**

Ageas reasonably expects to acquire.

Assumptions:

- Industry is a relevant factor to cyber exposure. 1
- SMEs' exposure indicates the SMEs' urgency to buy. 2
- Families will not spend more than 0.35% of their income.
- SMEs with high or total willingness to buy or to replace.
- Individuals with high or total willingness to buy.
- Ageas' market share (non-life branch) – SMEs.
- Market is equally distributed amongst players – families..

1 Industry is a relevant factor to cyber exposure.

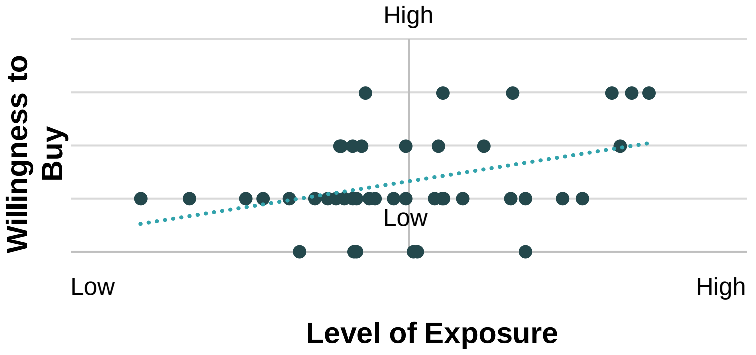
*"Beyond these unspecified threats, the relevance of other attack categories differs significantly, depending on the industry and the company's size and structure."*
**McKinsey, 2019**

*"Industry is the main segmentation criteria – the threats are targeted at certain industries"*
**Claranet**

*"Industry and size, for now, are good references for the level of cyber risk a company is exposed to."* **IDC**

Secondary data and industry experts interviews confirm this assumption.

2 SMEs' exposure indicates the SMEs' urgency to buy.




To confirm the assumption, we performed a correlation between the level of exposure of an SME and the willingness to buy (surveys data).

**Positive Correlation: *p-value=0.01***

**CURRENT MARKET:** Only SMEs operating in the most affected industries.

**POTENTIAL MARKET:** SMEs operating in the most and least affected industries.

- Assuming that firms are moving towards digital transformation, they will be more exposed to cyber risks.

## Methodology (Method 1)

**Calculate the no. of Portuguese SMEs with high and low exposure (according to industry)**

**SOURCES:**

INSTITUTO NACIONAL DE ESTATÍSTICA STATISTICS PORTUGAL · PORDATA · Orbis · verizon · NAICS

### 1 INE Criteria for SMEs

| | Small Enterprise | Medium Enterprise |
|---|---|---|
| Operating Revenues | € 2M - € 10M | €10M - €50M |
| | **OR** | **AND** |
| No. of Employees | 10-50 | 50-250 |
| PORDATA (2018) | **42.58K** | **6.96K** |

### 2 Industries – level of cyber exposure

Verizon's "Data Breach Investigation Report 2020" assessed 157.7K incidents and 32K passed the quality standards. These were compiled in a table by victims' industries – North America Industry Classification System (NAICS) – and company size (small, large, unknown).

| Most Affected Sectors | Least Affected Sectors | Excluded (potential partners or competitors) |
|---|---|---|
| 22 (Utilities)<br>31-33 (Manufacturing)<br>44-45 (Retail Trade)<br>48-49 (Transportation and Warehousing)<br>51 (Information)<br>52 (Finance and Insurance)<br>54 (Professional, Scientific, and Technical)<br>61 (Educational Services)<br>62 (Health Care and Social Assistance)<br>71 (Arts, Entertainment, and Recreation)<br>72 (Accommodation and Food Services)<br>92 (Public Administration) | 11(Agriculture, Forestry, Fishing and Hunting)<br>21 (Mining, Quarrying, and Oil and Gas Extraction)<br>23 (Construction)<br>42 (Wholesale Trade)<br>53 (Real Estate)<br>55 (Management Services)<br>56 (Administrative)<br>81 (Other Services) | 518 – Data processing, hosting and related services<br>524 – Insurance Carriers and Related Carriers<br>5415 – Computer Systems Design and Related Services<br>54169 – Other Scientific and Technical Consulting Services<br>5612 – Facilities Support Services |
| **25.36K**<br>(Current Market) | **21.68K**<br>(Potential Market) | **1.01K** |

### 3 No. of Portuguese SMEs from most and least affected sectors

Orbis database has detailed information about the companies. The filters applied were:

- Location: Portugal
- Status: Active and Unknown
- Operating Revenues and No. of Employees: SMEs (INE criteria)
- Activity and Industry: NAICS 2017 Code

There were **48.1K** of results which represents 97% of SMEs (2018).

### 4 Annual Growth Rate (2020-2025)

The geometric average of the annual growth rate of SMEs from 2014 to 2018 (PORDATA).

| Annual Growth Rate (20xx) | | | |
|---|---|---|---|
| 14-15 | 15-16 | 16-17 | 17-18 |
| 4.4% | 3.8% | 4.6% | 5% |

AGR: **4.45%**

## Methodology (Method 1)

1 Forecast the **VOLUME**

**Total Available Market**

SMEs and families with the need & financial ability to buy cyber insurance

Willingness to buy or replace

**Serviceable Available Market**

SMEs and families with or willing to buy for a cyber insurance

Market Share

**Serviceable Obtainable Market**

Ageas reasonably expects to acquire.

Assumptions:

- Industry is a relevant factor to cyber exposure.
- SMEs' exposure indicates the SMEs' urgency to buy.
- Families will not spend more than 0.35% of their income 3

- SMEs with high or total willingness to buy or to replace.
- Individuals with high or total willingness to buy.

- Ageas' market share (non-life branch) – SMEs.
- Market is equally distributed amongst players – families.

3 Families will not spend more than 0.35% of their income

INE: Household Expenditure Survey 2015/2016

- The average total annual household expenditure is €20.4K, from which €409 is spent on insurances – 2% of the total.

The majority of €409 is spent on the most common – and sometimes mandatory insurances (car, home, life).

According to the presented secondary data, the assumption is reasonable.

**Calculate the no. of households that have the financial ability to buy cyber insurance.**

1 No. of households with financial ability to buy cyber insurance

- The average price of family cyber insurance is €66. Thus, households with an annual income lower than €19K will not have the financial ability to buy cyber insurance.

**SOURCE:**

PORDATA

| Households by annual Income (2018) | | |
|---|---|---|
| Intervals | Less than €19K | More than €19K |
| Households | 9.05 M | 1.56M |

2 Annual Growth Rate (2020-2025)

The geometric average of the annual growth rate of SMEs from 2012 to 2018 (PORDATA).

| Annual Growth Rate (20xx) | | | | | |
|---|---|---|---|---|---|
| 12-13 | 13-14 | 14-15 | 15-16 | 16-17 | 17-18 |
| 2.8% | 0.3% | 2.8% | 5.3% | 5.8% | 6% |

AGR: **3.80%**

## Methodology (Method 1)

1 Forecast the **VOLUME**

**Total Available Market**

SMEs and families with the need & financial ability to buy cyber insurance

Willingness to buy or replace

**Serviceable Available Market**

SMEs and families with or willing to buy for a cyber insurance

Market Share

**Serviceable Obtainable Market**

Ageas reasonably expects to acquire.

Assumptions:

- Industry is a relevant factor to cyber exposure.
- SMEs' exposure indicates the SMEs' urgency to buy.
- Families will not spend more than 0.35% of their income.
- SMEs with high or total willingness to buy or to replace. 4
- Individuals with high or total willingness to buy.
- Ageas' market share (non-life branch) – SMEs.
- Market is equally distributed amongst players – families.

1 SMEs with high or total willingness to buy or to replace cyber insurance

**SOURCE:**

Surveys

47 SMEs

| SMEs with cyber insurance Willingness to Replace? | |
|---|---|
| Yes | 1 |
| Maybe | 4 |
| No | 4 |

| SMEs without cyber insurance Willingness to Buy | |
|---|---|
| Total | 1 |
| High | 8 |
| Some | 23 |
| None | 6 |

$$WTB = \frac{5+9}{47} = 30\%$$

4 SMEs with high or total willingness to buy or to replace.

**SECONDARY DATA - EUROSTAT**

Portuguese SMEs having insurance against ICT security incidents (2019): 9%

The lack of data – concerning SMEs willingness to adopt cyber insurance – lead the team to assess this issue through a survey.

**SURVEY**

Questions asked to survey respondents:

- *Does the SME has cyber insurance?*
- *If yes, is the firm willing to replace?*
  Answers: Yes, Maybe, No
- *If no, what is the firm willingness to buy?*
  Answers: Total, High, Some, None

The SMEs considered in the serviceable available market were the ones that answered high or total willingness to buy, to take into account respondents' tendency to respond positively to surveys.

## Methodology (Method 1)

1 Forecast the **VOLUME**

**Total Available Market**

SMEs and families with the need & financial ability to buy cyber insurance

Willingness to buy or replace

**Serviceable Available Market**

SMEs and families with or willing to buy for a cyber insurance

Market Share

**Serviceable Obtainable Market**

Ageas reasonably expects to acquire.

Assumptions:

- Industry is a relevant factor to cyber exposure.
- SMEs' exposure indicates the SMEs' urgency to buy.
- Families will not spend more than 0.35% of their income.

- SMEs with high or total willingness to buy or to replace.
- Individuals with high or total willingness to buy. 5

- Ageas' market share (non-life branch) – SMEs.
- Market is equally distributed amongst players – families.

1 Families with high or total willingness to buy cyber insurance

**SOURCE:**

Surveys

**525**

| SMEs without cyber insurance Willingness to Buy | |
|---|---|
| Total | 11 |
| High | 41 |
| Some | 293 |
| None | 180 |

$$WTB = \frac{11 + 41}{525} = 10\%$$

5 Individuals with high or total willingness to buy.

The lack of data – concerning families' willingness to adopt cyber insurance – lead the team to assess this issue through a survey.

**SURVEY**

Questions asked to survey respondents:

- *Do you have cyber insurance?*
- *If yes, is the firm willing to replace?*
  Answers: Yes, Maybe, No
- *If no, what is the firm willingness to buy?*
- Answers: Total, High, Some, None

Note: All respondents stated that they do not have cyber insurance.

The families considered in the serviceable available market were the ones that answered high or total willingness to buy, to take into account respondents' tendency to respond positively to surveys.

## Methodology (Method 1)

1 Forecast the **VOLUME**

**Total Available Market**

SMEs and families with the need & financial ability to buy cyber insurance

Willingness to buy or replace

**Serviceable Available Market**

SMEs and families with or willing to buy for a cyber insurance

Market Share

**Serviceable Obtainable Market**

Ageas reasonably expects to acquire.

Assumptions:

- Industry is a relevant factor to cyber exposure.
- SMEs' exposure indicates the SMEs' urgency to buy.
- Families will not spend more than 0.35% of their income.

- SMEs with high or total willingness to buy or to replace.
- Individuals with high or total willingness to buy.

- Ageas' market share (non-life branch) – SMEs. 6
- Market is equally distributed amongst players – families. 7

1 Ageas' Market Share (Cyber Insurance) – SMEs

**SOURCE:** Internal Company Data

ageas portugal Market Share (Non-Life) 〉 **13.8%**

2 Ageas' Market Share (Cyber Insurance) – families.

Players: FIDELIDADE, Inter Partner Assistance, ageas portugal, **NEW (?)**

$$Market\ Share = \frac{100\%}{4} = 25\%$$

6 Ageas' market share (non-life branch) for SMEs

Cyber insurance is in its growth stage, and the market is only composed of 13 players. Moreover, there is an untapped demand for tailored solutions. Thus, the team discussed with the client this premise that assumes that Ageas' market share in cyber insurance would be the same as in the non-life branch. After pondering, the assumption was considered reasonable.

7 Market is equally distributed amongst players

There are only two competitors in the personal cyber insurance market. Thus, the team assumed that a new player (other than Ageas) may enter the market and that market shares will be equally distributed amongst players,

Note: Due to lack of data, the team could not find a more reasonable assumption.

## Methodology (Method 1)

2 Forecast the **PRICE** 〉 WTP from respondents considered in serviceable available market 1

1 WTP from respondents considered in SAM

To forecast the price, the team calculated the average annual premium that respondents – considered in the serviceable available market – are willing to pay for cyber insurance.

**Calculate the average annual premium – WTP**

1 For SMEs

**SOURCE:** Surveys

**14 SMEs**

high or total willingness to buy cyber insurance or replace

| SMEs with cyber insurance | |
|---|---|
| Less than €750 | 1 |
| €1 500 - €3 000 | 2 |
| €3 000 - €6 000 | 1 |
| Do not Know | 1 |

| SMEs without cyber insurance | |
|---|---|
| Less than €750 | 2 |
| €750 - €1 500 | 5 |
| €3 000 - €6 000 | 2 |

The team considered mean value of the price ranges:

| | |
|---|---|
| €750 | 23.1% |
| €1 125 | 38.5% |
| €2 250 | 15.4% |
| €4 500 | 23.1% |

Average Annual Premium:
**€ 1 990**

2 For Individuals

**SOURCE:** Surveys

**52**

high or total willingness to buy cyber insurance

| Families | |
|---|---|
| Less than €40 | 10 |
| €40-€60 | 10 |
| €60-€80 | 13 |
| €80-€100 | 14 |
| More than €100 | 2 |

| Families | |
|---|---|
| €40 | 19% |
| €50 | 25% |
| €70 | 25% |
| €90 | 27% |
| €100 | 4% |

The team considered mean value of the price ranges

Average Annual Premium:
**€ 66**

[1]McKinsey and Verizon

## Methodology (Method 1)

3 Consider Market Evolution

Current Market Size: 2020

Potential Market Size: 2025*

- SMEs WTB = % of Spanish SMEs with cyber insurance (2019) 1
- Families' WTB = % of respondents with paid online protection 2

### 1 SMEs WTB = % of Spanish SMEs with cyber insurance (2019)

The Portuguese cyber insurance market is expected to grow and thus, it is reasonable to assume that SMEs' willingness to buy will move towards the Spanish current reality.

### 2 Families' WTB = % of respondents with paid online protection

Ageas' cyber insurance will include online protection. Moreover, the personal cyber insurance market is also expected to grow. Thus, it is reasonable to assume that families' WTB will move towards the current willingness to buy online protection.

### 1 SMEs WTB's for the potential market (in 2025)

**SOURCE:**

Secondary Data

eurostat

% of Spanish SMEs having insurance against ICT security incidents (2019)

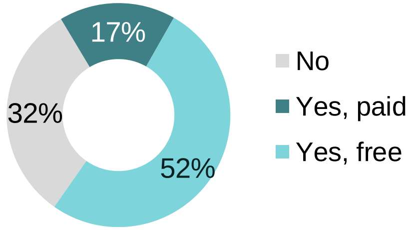
WTB: **32%**

### 2 Families WTB's for the potential market (in 2025)

**SOURCE:**
Surveys

525

Do you have online protection in your personal devices?




WTB: **17%**

[1]McKinsey and Verizon

## Methodology (Method 2)

### Using Italy's publicly available data on Cyber Insurance to extrapolate Portugal's values:

1

| | |
|---|---|
| Cyber Insurance Market Value Italy (M€, 2017) | 20 |

28% (AGR)

| | |
|---|---|
| Cyber Insurance Market Value Italy (M€, 2020) | 41.94 |

### Cyber-attack rates (CAR) (% of attacked machines), 2019

4

| | CAR (%) | CRI (M. €) |
|---|---|---|
| Italy | 4.19% | 41.94 |
| Portugal | 3.83% | ? |

| | CAR (%) | CRI (M. €) |
|---|---|---|
| Italy | 4.19% | 41.94 |
| Portugal | 3.83% | 38.34 |

### Gross Domestic Product (GDP), 2019

2

| | GDP (Bn. €) | CRI (M. €) |
|---|---|---|
| Italy | 1 721.06 | 41.94 |
| Portugal | 204.41 | ? |

| | GDP (Bn. €) | CRI (M. €) |
|---|---|---|
| Italy | 1 721.06 | 41.94 |
| Portugal | 204.41 | 4.98* |

$* \frac{41.94M\ € \times 204.41bn\ €}{1721.06\ bn\ €}$

### ITU Global Cybersecurity Index (GCI), 2018

3

| | CGI | CRI (M. €) |
|---|---|---|
| Italy | 0.84 | 41.94 |
| Portugal | 0.76 | ? |

| | CGI | CRI (M. €) |
|---|---|---|
| Italy | 0.84 | 41.94 |
| Portugal | 0.76 | 37.98 |

### Weighted average between the three variables chosen:

| Variables | Portuguese Cyber Risk Insurance Market Estimates (M. €) | Weights |
|---|---|---|
| **GDP** | 4.98 | 10% |
| **ITU GCI** | 37.98 | 40% |
| **Cyber attack rate** | 38.34 | 50% |
| | | 100% |

| | |
|---|---|
| Estimation of the total Portuguese Cyber-Risk Insurance Market (without adjustments) | € 34.86 M |

***Sources**: Enterprise Ireland (Global Ambition); ITU; World Development Indicators; OECD*

Back to Presentation

## Methodology (Method 2)

### Weighted average between the three variables chosen and Purchasing Power Parity (PPP) Portugal/Italy

| | |
|---|---|
| Total Portuguese Cyber Risk Insurance Market Estimate (without adjustments) | € 34.86 M |
| PPP (2018) Portugal/Italy | 0.848 |

### Distribution between commercial (B2B) and personal (B2C) Cyber Insurance Market Value

| | US $ (bn.) | € (bn.) | % |
|---|---|---|---|
| Global Cyber Insurance Market Value | 7.50 | 6.45 | 100 |
| *Commercial Cyber Insurance Market Value | 4.50 | 3.87 | 60 |
| Personal Cyber Insurance Market Value | 3 | 2.58 | 40 |

*Includes all-sized companies

### B2B
Large
SMEs
Micro

Only SMEs

| Calculated SOM (value) | € 2.1 M | In Million Euros (€) |
|---|---|---|
| Portuguese B2B Cyber Insurance Market Estimate (34.86M x 60%) | | 20.92 |
| Adjusted PPP (Portugal/Italy) | | 17.73 |
| **Obtainable Ageas B2B Cyber Insurance Market Estimate** (Considering 13.8% Market Share) | | **2.5*** |

*Also Includes large and micro companies

### B2C

| Calculated SOM (value) | € 2.6 M | In Million Euros (€) |
|---|---|---|
| Portuguese B2C Cyber Insurance Market Estimate (34.86M x 40%) | | 13.94 |
| Adjusted PPP (Portugal/Italy) | | 11.82 |
| **Obtainable Ageas B2C Cyber Insurance Market Estimate** (Considering 25% Market Share) | | **3.0** |

***Sources**: KPMG, Swiss RE, OECD*

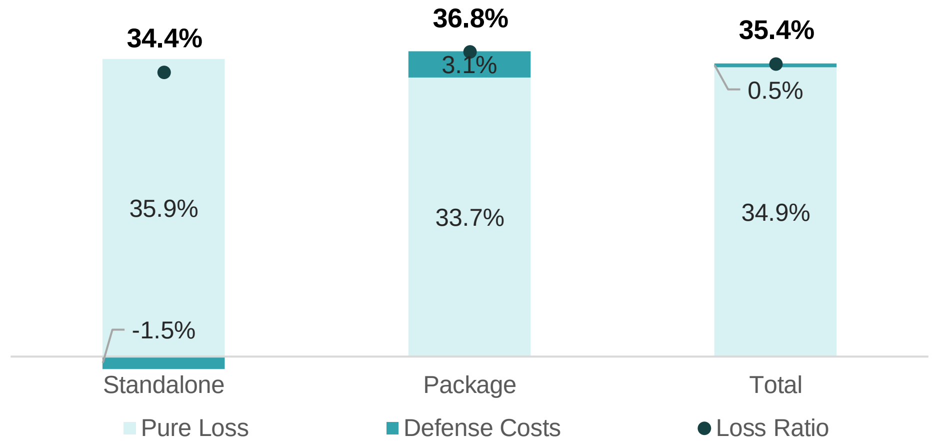
## Agenda

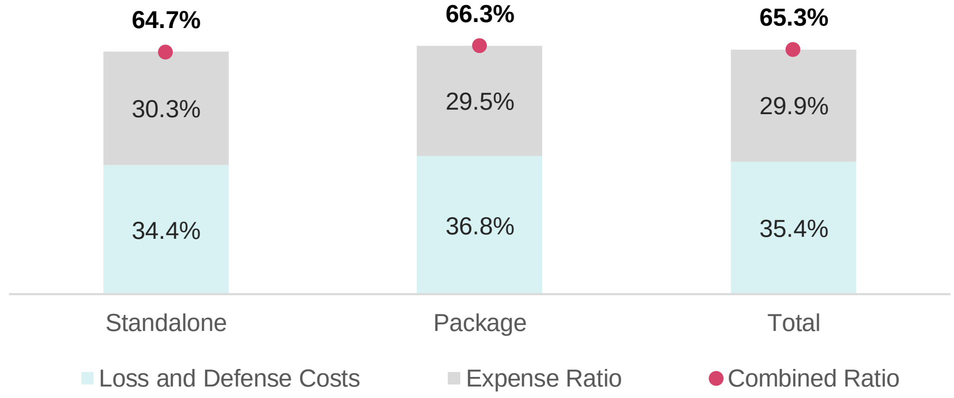
# APPENDIX 5 – CLAIMS RATIOS

Back to Presentation

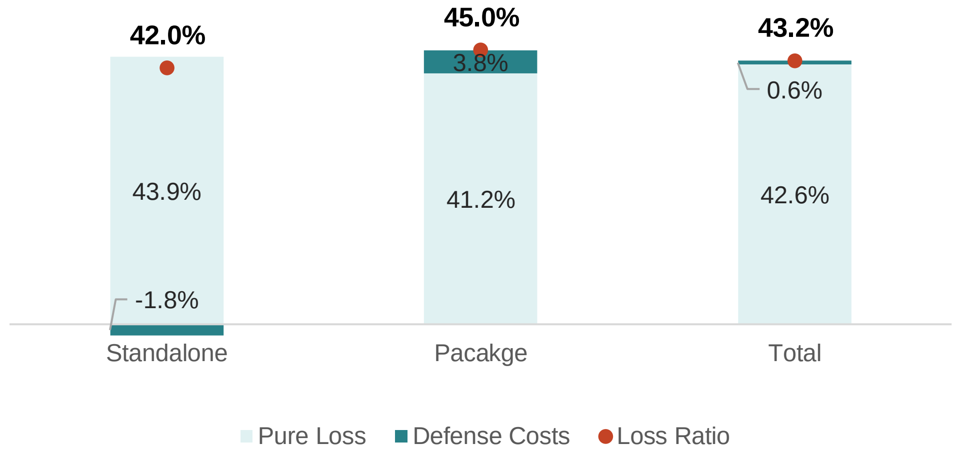
| | Loss Ratio | Combined Ratio |
|---|---|---|

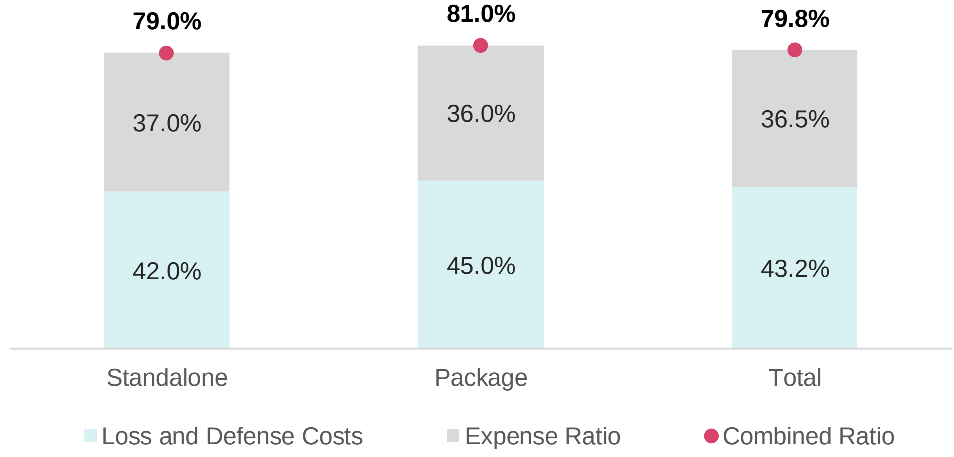
**United States**




**Portugal**




***Sources**: Aon, ITU*

## Agenda

For Benchmarking and BPs Analysis, the team chose the most developed market worldwide (USA) and the most mature markets in Europe (UK, Germany, and Spain). In these European countries, national insurance associations have created cyber-resilience initiatives that will support cyber insurance companies and increase national cyber awareness.

## Global Cyber Insurance Market

| Top 5 Market Share, 2018 | Benchmarking and BPs Analysis |
|---|---|
| USA | Most developed market worldwide |
| China | Non-comparable due to regulatory discrepancies |
| UK, Germany, Spain | Most mature EU markets |

### Cyber-resilience initiatives by European national insurance associations

**These initiatives increase national cyber awareness and support cyber insurance companies.**

**United Kingdom**

- The NCSC operates a "Cybersecurity Information Sharing Partnership" that allows the government and the private sector to exchange cyber-threat information in real time.
- Cyber Insurance Forum: regular meetings between insurance representatives and government officials to discuss challenges facing cyber insurance.

**Germany**

- The GDV published non-biding wording for cyber insurance for SMEs.
- The GDV developed an online free risk assessment tool for potential commercial insurance buyers.
- The GDV is collecting data on market developments relating to cyber insurance for insurers.

**Spain**

- UNESPA, Cepreven, and Cepyme have developed a free guide "Cyber risk: its impact on SMEs" which details measures to prevent and mitigate the damage of cybercrimes.

***Sources:*** *The Business Research Company, Insurance Europe*

## Cyber Insurance Market - USA

Major Players: CHUBB, AIG, AXA

### Key Insights

**OFFER & LEVEL OF CUSTOMIZATION**

- All 3 companies have more than one offer;
- 2 out of 3 companies have at least 1 customized offer;
- Most offers target all-size enterprises while offering different products to target industries.

**PREVENTION**

- All perform risk assessment and regulatory compliance evaluation;

**PROTECTION**

- Most of the standalone products guarantee protection services, namely employee education, AV protection software, back-up system configuration, and end-point security system

**PREPARATION**

- 8 out of 11 offers guarantee incident response planning and review;

**POST-ASSISTANCE**

- First-party coverage: all standalone products offer compensation for first-party software damages, data restoring, forensic work, business interruption, and reputational harm;
- Third-party coverage: all offers guarantee compensation regarding litigation and regulatory fines as well as third-party communications and notifications and breach of privacy and confidence.

### Best Practices

| | |
|---|---|
| CHUBB | Chubb is the first insurer in the industry to cover:<br>• Protection against **cyberbullying** - included in housing cyber insurance, namely assistance in dealing with online harassment that results in wrongful termination or emotional impact;<br>• Protection against **cyber disruption** - support dealing with cyberattacks that prohibit the access to client's home, or attacks interrupting a small owned business. |
| AIG | • **CyberEdge Plus** is a complement to CyberEdge insurance to respond to any physical damages, in terms of property and people, in consequence of a cyber attack.<br>• Offers a **risk assessment tool** (CyberEdge RiskTool) assuring security, training, and compliance. The security module offers a hardware tool (AutoShun) to prevent cyber attacks. |
| AXA | • **CyberRiskConnect.com** – platform where clients have access to AXA's online resources, to learn more about cyber-security readiness and IR service;<br>• **Claim Experts Team** - assistance to breach response with specialized teams available 24 hours a day, 7 days a week |

***Sources:** Chubb, AIG, AXA XL*

## Cyber Insurance Market – UK

**Major Players**: HISCOX, beazley, cfc

### Key Insights

**OFFER & LEVEL OF CUSTOMIZATION**

- All three companies offer more than one product;
- 8 out of 11 insurance products are standardized;
- All companies target all-size companies, offering different insurance products for specific industries

**PREVENTION**

- All companies perform risk assessment and only 1 out of 3 companies perform Regulatory Compliance Evaluation (Beazley);

**PROTECTION**

- Only 1 out of 3 companies (Beazley) offers comprehensive risk mitigation services.

**PREPARATION**

- All insurers offer Incident Response Planning and Review, while only 1 performs Penetration Tests;

**POST-ASSISTANCE**

- First-party coverage: all offers guarantee compensation for software damages, data restoring, business interruption, and reputational harm;
- Third-party coverage: all offers guarantee compensation for litigation and regulatory fines and breach of privacy and confidence.

### Best Practices

| | |
|---|---|
| HISCOX | • **Repeat event mitigation:** the insurer will pay reasonable and necessary costs only if the company agrees to:<br>1. Upgrade existing hardware or software forming part of the company's computer system;<br>2. Obtain risk management advice - the insurer provides this service outsourced.<br>• **"Build my Cover" functionality:** the client answers a few questions online about its business such as: industry; turnover; number of employees and the program generates an appropriate coverage. |
| beazley | • **BRB team:** internal team in the company responsible for BBR policyholders at every stage of incident investigation and breach response (in partnership with Lodestone Security);<br>• **Claims and Underwriting teams** are specific to cyber risk. |
| cfc | **Partnerships for risk awareness and mitigation:**<br>• **CyberRiskAware**: e-learning tool that tackles human vulnerabilities in a business, providing training on how to identify and prevent phishing attacks;<br>• **Ninjio**: library with fun and engaging cyber risk awareness videos, covering a wide range of scenarios;<br>• **Cyber Risk Rating Report:** outsourced service to Bitshight that reviews companies' risk exposure, benchmarking them to their peers and competitors. |

***Sources:*** *Hiscox, Beazley, CFC Underwriting*

## Cyber Insurance Market - Germany

**Major Players**: Basler Versicherungen; PROVINZIAL – Die Versicherung der Sparkassen; MARKEL

### Cyber Insurance Rating

Franke | Bornberg

Very high level of detail: only hard, comprehensible facts that are valid for the entire duration of the contract are evaluated.
FFF+ (excellent) to F- (unsatisfactory)

### Key Insights

**OFFER & LEVEL OF CUSTOMIZATION**

- Only one product per company;
- All companies have their offers within a framework of selectable modules;
- Most offers focus on SMEs and one is specialized for freelancers and intermediates.

**PREVENTION**

- All perform risk assessments, but none of them refer to regulatory compliance evaluation.

**PROTECTION**

- Only one offer guarantees risk mitigation measures.

**PREPARATION**

- Only one offer guarantees incident response planning and review and penetration testing.

**POST-ASSISTANCE**

- All insurances offer complete first-party coverage. Only 1 includes dependent business interruption;
- All insurances offer complete third-party coverage. Only 1 includes multimedia liability coverage.

### Best Practices

**Basler Versicherungen**

**24 hotline Support**: Specialized IT experts on the phone provide direct assistance. They connect to the enterprise's system via remote maintenance and thus solve most problems.

**PROVINZIAL – Die Versicherung der Sparkassen**

**Cyber Check**: the client answers 39 questions on security-related topics. At the end receives a matrix, which shows the risk situation of the company. Moreover, the client has the option to add further data and receive a detailed PDF report.

| Themenkomplex | Kategorie | | | |
|---|---|---|---|---|
| Organisation | Organisation der Informationssicherheit | Richtlinien | Personal | Zugänge |
| | 50% | 50% | 50% | 0% |
| Technik | Mobile Geräte | Mobile Datenträger | Netzwerke | IT-Systeme |
| | 50% | 100% | 67% | 50% |
| Prävention | Sicherheitsvorfälle | Umgebung | Datensicherung | Ausfälle |
| | 67% | 0% | 33% | 50% |
| Management | IT-Outsourcing und Cloud Computing | | | |
| | 100% | | | |

**MARKEL**

**Modular framework with 8 flexible optional building blocks:**

- Cyber and intrinsic data damage
- Cyber business interruption
- Cyber extortion
- Cyber payment means
- Cyber fidelity damage
- Cyber liability
- Cyber prevention premium

***Sources:*** *Basler Versicheringen, Provinzial, Markel*

Back to Presentation

# Cyber Insurance Market - Spain

**Major Players**: MAPFRE, Allianz, Catalana Occidente (Grupo asegurador)

## Key Insights

**OFFER & LEVEL OF CUSTOMIZATION**

- Only one product per company;
- 2 out of 3 companies have a customized offer;
- Most offers target all-size enterprises and two of them target freelancers.

**PREVENTION**

- All perform risk assessment and 2 of them perform regulatory compliance evaluation.

**PROTECTION**

- 2 offers guarantee protection services, including employee education, AV protection software, and back-up system configuration.

**PREPARATION**

- 2 offers guarantee incident response planning and review.

**POST-ASSISTANCE**

- First-party coverage: all offers guarantee compensation for software damages, data restoring, business interruption, and reputational harm;
- Third-party coverage: all offers guarantee compensation for litigation and regulatory fines and breach of privacy and confidence.

## Best Practices

Catalana Occidente Grupo asegurador; Allianz

**Cyber risk Web Page:** both of these companies offer a Cyber Portal, exclusive to their insured clients, to manage risk (including compliance tools) and report its cyber incidents.

**Catalana Occidente:** Portal Ciberriesgos

**Allianz:** Platorma Digital de Autoservicio

**Main features:**

- Interactive digital platform specialized in cybersecurity that allows online and integrated management of the contracted services;
- Direct contact channel that responds to companies' questions and needs, attended by experts who solve all doubts, requirements and listen to complaints;
- Specialized services with the capacity to act;
- 24-hour coverage in the event of a cyber attack.

*Sources: MAPFRE, Allianz, Catalana Ocidente*

## Agenda

# APPENDIX 7 – SWOT and TOWS ANALYSES (I/III)

## ✓ STRENGHTS

- ✓ **Solid client base** – 1,7M customers (2nd largest insurance group in Portugal) - allows for a successful product development strategy (new product to existing market)
- ✓ **Extensive ecosystem** with insurance and beyond insurance services that can be complemented with a new cyber risk offering
- ✓ **Strong due diligence** and **negotiation** capabilities
- ✓ **Technology and innovation-driven culture** can facilitate the development of the cyber risk value proposition
- ✓ **Robust financial situation** – a positive net result of €110M and a combined ratio of 88,4% - providing the required flexibility to pursue high risk and high commitment investments

## ✗ WEANESSES

- ✗ **High level of commitment of the company** – necessary investments in human capital and in establishing partnerships - for a considerable level of risk
- ✗ **Limited specialization**, knowledge, and experience on cybersecurity constraining the capacity to manage the new offering:
  - ✗ **Lack of historical data** specific to cyber risk limits the development of a cyber underwriting model
  - ✗ **Absence of technical expertise** on cybersecurity-related departments – IT, forensic, legal, communications & notifications, PR and IR teams

***Sources**: Grupo Ageas Portugal*

## OPPORTUNITIES (I/II)

**Digitalization**, for both individuals and enterprises, has led to a **brisk evolution** of cyber risks.

- **Shift towards a digital economy:** a trustworthy digital economy is critical to their organization's future growth (according to 90% of business leaders), but the drive for digital innovation is introducing new risks.

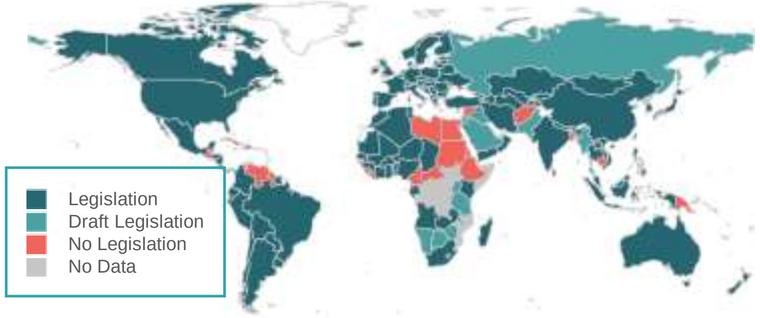
| 25% \| 100% (2005 \| NOW) | Cloud-based services & 5G | 80% |
|---|---|---|
| of companies rely on the Internet for their business operations | expanding cyber attacks' opportunities along the entire supply chain | of companies introducing digital innovation faster than their ability to secure it |

- **Shift towards the digital world:** Over the years, the Internet has made individuals' lives easier and faster, causing its usage to be rapidly and continuously increasing. However, this dependency also brings new risks:

| 1.100M \| 4.131M (2005 \| NOW) | 3.960M | 56% |
|---|---|---|
| users on the Internet - 275.54% increase | people use any type of social media | of internet users were estimated to have experienced any cyber crime |

Cyber-security and data protection **laws** have an **ambiguous** effect on cyber risk

- Rapidly evolving **regulations catalyze** improvements of cyber risk **awareness** and mitigation




**66%** With Legislation

**19%** Without Legislation

- In the event of a cyber incident, current **legal obligations** originate **additional losses** (fines and compensation costs)

**General Data Protection Regulation (GDPR)**

| Lower Level | | Upper Level | |
|---|---|---|---|
| €10M | 2% of global turnover | €20M | 4% of global turnover |

**Sources:** *Accenture, Data Privacy Manager, Statista, UNCTAD*

Back to Presentation

## OPPORTUNITIES (I/II)

- Mismatch between client's needs and cyber insurer's offers, creating an **untapped demand for differentiated solutions**

The urge for **increasingly tailored and extensive insurances** creates untapped demand with a considerable market size:

**SMEs**

SMEs represent the **highest potential for cyber insurers** since:

- Are less protected by cyber insurances than large enterprises – thus becoming the most attractive target for cybercriminals.
- Have less financial flexibility to recover from a cyber attack.

## THREATS

- Influx of **new entrants** due to high profitability and significant growth potential:

**12%** Increase of US cyber insurers – 2018

**45%** Low Loss Ratio (US, 2018)

- **Alternative coverage** solutions can disrupt the industry:

**Self Insurance**
Either by creating cyber risk reserve funds or securitizing the risk by floating cyber bonds in the capital markets

**Insurer Techs**

- Cyber policies remain overly **standardized** and **limited** due to:

✓ Short supply of skilled workers

**33%** Increase of new cybersecurity programs

**94%** Increase in cybersecurity jobs

✓ Limited application of standard actuarial techniques:

Data scarcity (quantity and quality)

Changing risk dynamics

***Sources**: Insurance Journal, AON, Deloitte, Munich RE*

## Agenda

## Cybersecurity and IT Providers and Consultants for B2B Segment (I/III)

**1. Cyber Risk Definition:**

- How do you define cyber risk – for individuals and enterprises/organizations?
- How do you categorize cyber risks – according to the activity (e.g. criminal versus non-criminal), type of attack (e.g. malware, DDoS, etc.), source of the risk (e.g. terrorisms, criminals, government).
- Which types of consequences from cyber incidents do you consider – for enterprises and individuals.
    - Tangible losses – business interruption costs, computer-related assets (hardware, software, data) recovery costs, compensation for breach of confidence/privacy, regulatory/litigation costs, communications/public relations/notifications expenses?
    - Intangible losses (reputational damage – customer turnover, increased costs of customer acquisition; human impacts – psychological and physical).

**2. Market: The dynamic changes in cyber risk (due to fast-changing technology innovations, the rapidly evolving legal landscape, and the current pandemic situation) contribute to asymmetric information.**

- What is the current market situation compared to the other European countries – high, medium, or low maturity?
- What is the level (high, medium, low) of cyber awareness and readiness in Portugal – for enterprises/organizations and individuals?
- Can you identify other factors influencing the maturity level of the Portuguese (e.g. short supply of skilled workers)?
- Considering the previously mentioned external factors, what is the current market size versus the market potential of cyber risk in Portugal?

**3. Customer Segments:**

- What are the segmentation criteria – for enterprises (e.g. industry, size) and individuals (public exposure, children).
- Which segments represent the most potential and which factors contribute to the attractiveness of these segments?

## Cybersecurity and IT Providers and Consultants for B2B Segment (II/III)

**4. Offering (product and service):**

- What is the product scope of your cyber risk offering? – does it includes prevention (risk assessment), protection (risk mitigation), preparation (contingency and monitoring plans), and post-incident (risk transfer – coverage of tangible/intangible losses) services?
- Which services does risk assessment include? – information value appraisal, ICT cybersecurity analysis, regulatory compliance evaluation?
- Which services does risk mitigation include? – employee education, updates and upgrades of software, install AV protection software, back-up system configuration, endpoint security system, secure external web-facing servers and applications, multi-factor authentication?
- Which services do contingency and monitoring plans include? – monitor network traffic, penetration testing, incident response planning, and review?
- Which services do risk transfer coverages include?
- What is the level of customization of the offering?

**5. Vertical Integration:** The dynamism of the industry implies a constant improvement of the offerings provided by cyber risk suppliers so that the products and services can satisfy clients' needs. Thus, we believe that the cyber risk industry is evolving towards a collaborative ecosystem, where there is a thin line separating indirect competitors from potential partners, that will benefit from knowledge and information sharing. For instance, cybersecurity/IT providers possess the technical skills and experience to perform risk assessment and mitigation; cybersecurity/IT consultants capitalize on a large customer network and know-how on monitoring and contingency plans; cyber insurers possess underwriting and claim management capabilities (risk transfer).

- What is the competitive advantage – how does the company adds differentiated value to the cyber risk value proposition?
- What activities are outsourced? Why? Through which collaborative partners?
- What is the advantage of partnering up with a cybersecurity consultant versus cyber insurance? (for cybersecurity providers)
- What is the advantage of partnering up with a cybersecurity provider versus cyber insurance? (for cybersecurity consultants)

## Cybersecurity and IT Providers and Consultants for B2B Segment (III/III)

- If the company is partnering with a cyber insurer:
- What is the average risk percentage they hold when they reinsure?

**6. Channels:** In terms of marketing and distributing your offerings, how would you divide the weight between online and offline channels? (i.e. what overall percentage of sales are completed through the website and/or social media versus in-store)

**7. Pricing**

- What is the correlation between the costs of services offered and the level of cyber risk? (e.g. higher costs for riskier industries/enterprises)
- How is this correlation reflected in pricing?

## Professors (I/II)

**1. Cyber Risk Definition:**

- How do you define cyber risk – for individuals and for enterprises/organizations?
- How do you categorize cyber risks – according to the activity (e.g. criminal versus non-criminal), type of attack (e.g. malware, DDoS, etc.), source of the risk (e.g. terrorisms, criminals, government).
- Which types of consequences from cyber incidents do you consider – for enterprises and individuals.
    - Tangible losses – business interruption costs, computer-related assets (hardware, software, data) recovery costs, compensation for breach of confidence/privacy, regulatory/litigation costs, communications/public relations/notifications expenses?
    - Intangible losses (reputational damage – customer turnover, increased costs of customer acquisition; human impacts – psychological and physical).

**2. Evolution of Cybercrimes**

- What are the most frequent cyber risks - for individuals and SMEs?
- How do you foresee the evolution of cybercrime and the prevention and mitigation of this type of crime in the coming years? In this sense, do you project that risks will stabilize or continue to increase (due to the inability to respond to increasingly sophisticated cyber attacks)? What external factors will be decisive for this evolution?

**3. Evolution of the Cybersecurity Market**

- What is the current situation of the cybersecurity market compared to other European countries and worldwide (high, medium, or low maturity)?
- What are the factors that explain this situation and, specifically, what are the obstacles to the growth of this market in Portugal?

## Professors (II/II)

**4. Offer and potential of private cybersecurity initiatives:**

- What are the most advanced mechanisms (technology) on the market today to:
  - Risk assessment;
  - Preparation (Contingency Plans / Penetration tests)
  - Protection (Risk Mitigation);
  - Post assistance (data recovery, digital content recovery, etc.)
- Which companies/institutions in Portugal develop these mechanisms? And worldwide?
- Do you think that public institutions will have the capacity to respond to fully protect individuals and companies/organizations? If not, do you foresee an increasing demand for prevention, protection, and assistance services provided by private companies?
- In your opinion, are individuals and SMEs (specifically those with less than 250 employees) aware of the consequences (financial, reputational, and human) of cyber-attacks?
- How can private initiatives (i.e., cybersecurity companies, consultants, and insurers) increase public awareness of the dangers of cyber-attacks?
- Do you consider that there is potential for insurers to enter this market? Namely, establishing partnerships with cyber risk companies, outsourcing risk assessment, mitigation activities, and the technical part of post-assistance (data recovery, etc.), making the insurer responsible for legal issues and claims management.

## CNCS – National Centre of Cybersecurity (I/II)

**1. Cyber Risk Definition:**

- How do you define cyber risk – for individuals and enterprises/organizations?
- How do you categorize cyber risks – according to the activity (e.g. criminal versus non-criminal), type of attack (e.g. malware, DDoS, etc.), source of the risk (e.g. terrorisms, criminals, government).

**2. Evolution of Cybercrimes**

- How do you foresee the evolution of cybercrimes and their prevention and mitigation in the coming years?
- In this sense, do you project that risks will stabilize or continue to increase (due to the inability to respond to increasingly sophisticated cyber attacks)?
- What external factors will be decisive for this evolution?
- Do you think that public institutions will have the capacity to respond to fully protect individuals and companies / organizations? If not, do you foresee an increasing demand for prevention, protection and assistance services provided by private cybersecurity companies, consultants and / or insurance companies?

**3. CNCS Projects and Resources - Awareness and Readiness of the Portuguese Population**

- Regarding the Awareness and Training Project:
    - When organizing training, what are the responsibilities of CNCS and partners?
    - Can any entity establish a partnership with CNCS, to organize training for its employees?
    - Would you be willing to establish partnerships with cyber insurers - providing your resources to policyholders to increase the visibility of your resources and, consequently, boosting the population's awareness of cyber risks?

## CNCS – National Centre of Cybersecurity (II/II)

- Considering the participants of the e-learning course “Ciber Seguros” and the “Cibertemas” Seminars, are you able to obtain statistical information on the levels of awareness about cyber risks inherent to different segments?
    - Individuals - by gender, age, education level, income, etc.
    - Companies - by size (number of employees and turnover), sector, industry, etc.

**4. CNCS Projects and Resources - Awareness and Readiness of the Portuguese Population**

- CERT.PT is a service that is part of CNSC. From what we understand, it is the subdivision responsible for responding to incidents involving State entities.
- What are the main activities and responsibilities of this unit?

## Engineer José Galamba de Oliveira – President of APS (Portuguese Insurance Association)

**BACKGROUND:**

- The project has two main objectives:
    - Strategic assessment of the potential value for insurers at cyber risk.
    - Comprehensive approach to developing a successful value proposition.

**QUESTIONS:**

**Question 1:**

- What is the current situation of the cyber insurance market in Portugal - for companies and individuals? In particular, what are the main insights in relation to KPIs such as loss / combined ratios and frequency and severity of claims? Taking into account indirect competition (eg, IT and cybersecurity companies), how do you think Insurers can position themselves to add value to your proposal?

**Question 2:**

- The asymmetry of information, the scarcity of data (frequency and severity of claims), of specialized technicians, and the dynamic changes in cyber risk (due to rapid technological innovations and changes in the legal framework) challenge the traditional policy model. In addition, cyber insurance differs from usual products (eg housing, car) in that it includes additional prevention, protection, and post-accident assistance services.
- How can insurance companies overcome these challenges and what are their perspectives regarding the future of this market in Portugal?

**Question 3:**

- In the more mature European countries, national insurance associations have developed cyber resilience initiatives to raise awareness and support insurers that compete or plan to enter this market. For example, the German Insurance Association (GDV) has developed a free online risk assessment tool for potential cyber insurance buyers.
- Is the Portuguese Insurance Association (APS) developing a similar initiative or does it plan to do so in the near future?

## Agenda

**1. What do you think when you are referred to the following words: “cybersecurity”, “cyber attack”, “cyber risk”, “cybercrime”, etc.?**

**2. Can you identify the consequences of the cyber incidents you mentioned?**

**3. Has your organization ever been a victim of a cyber incident?**

If yes:

- How many times and how long ago?
- What was the type of cyber attack and its origin? In what context did it happen?
- What were the main consequences of this event?
- How was the situation managed?
- To whom did you report the incident? What assistance was provided to you?

If not:

- Do you consider that the company is likely to be a victim of this type of attack in the future? For any specific reason? (e.g., information sensitivity, company size - in terms of billing or employees, industry).
- Are you aware of any cyberattacks that have occurred on a competing company?
- What impact did it have on the company's perspective regarding cyber risks?

**4. Does the organization adopt cybersecurity measures? If so:**

- What are the preventive measures adopted by the company? (e.g., GDPR compliance assessment, vulnerability diagnosis)
- What are the protection measures? (e.g., the security of information systems infrastructure, back-up plans (i.e., back-up copies), employee training)
- What are the contingency and monitoring measures? (e.g., incident response plan, purple teams)
- Are cybersecurity services internal or provided through partnerships?
- Who is responsible for these decisions?

**5. Do you have cyber risk insurance?**

If yes:

- Is it an independent insurance or is it included in a multi-risk?
- Does it include prevention, protection, and preparation services? If so, which ones?
- What are the coverages (post claims)?
  - Tangible (business interruption, computer assets, information retrieval, compensation for breach of confidentiality / privacy, legal / regulation, communication / notification / public relations)
  - Intangibles (reputational + emotional).
- What were the criteria for choosing insurance?
  - Price;
  - Coverages;
  - Brand confidence;
- How did you purchase this insurance?
- Were you approached by an agent/mediator? If so, do you consider the advice of your agent/mediator to have a significant bearing on your decision?
- Did you find out at a counter?
- Did you find out on the insurer's online channels?
- Did you have to fulfil an application form?
  - If the person has children: what was your perception about filling in the application form? (duration, complexity, etc.).

If not:

- What are the reasons for not buying insurance?
  - Lack of awareness (e.g..: “We never thought about it”)
  - Lack of knowledge about the offer (e.g., “We would like to have cybersecurity, but we do not know how to obtain information about the offers on the market.”).
  - Lack of necessity (e.g., “The company does not have many risks” “The level of cybersecurity protects us in full against any possibility of loss.”, Etc.). Why?
  - Inaccessible prices.
- Has the organization considered the purchase? If so, what is the reason for not continuing?

**6. In recent times, have the words “cybersecurity”, “cyber-attack”, “cyber risks”, “cybercrimes” come up more often in your life?**

- If so, in what contexts and why? (i.e., + frequency, + severity or both).

**7. Do you consider that cybersecurity can gain relevance at the top of your company's priorities?**

- If so, do you think that the organization will be able to buy cyber risk insurance in the near future?

  If yes:

  - What are the main features you would be looking for?
  - Through which channel would you prefer to buy the insurance?
  - What monthly premium would they be willing to pay? Why?

# APPENDIX 9 – IN-DEPTH INTERVIEW GUIDE (B2C SEGMENT) – I/III

**1. What do you think when you are referred to the following words: “cybersecurity”, “cyber attack”, “cyber risk”, “cybercrime”, etc.?**

- What types of cybercrime do you know?
- Can you identify the consequences of the cybercrimes you mentioned? Which are?

**2. Has the “name” or someone in your household ever been a victim of cybercrime?**

If yes:

- How many times and for how long?
- What type of cybercrime and in what context did it happen?
- Who was the victim (son, husband, age, gender, occupation, education level)?
- What are the main consequences of this event - financial and emotional?

How was the situation managed?

• To whom did you report the incident? What assistance was provided to you?

If not:

- Do you consider that you or someone in your household is likely to be a victim of this type of crime in the future? For any specific reason? (e.g., professional, tech-savvy occupation).
- Are you aware of any cases of cyber attack?
- [If the person has minor children and do not mention cases of cyberbullying]:

• How do you define cyberbullying?

- Do you think there is a strong chance that one of your children will be a victim of cyberbullying in the future?
- Are you aware of any victim of cyberbullying?

If yes: Was the abuser a colleague or an adult? What impact did this event have on your perspective on cyber risks?

**3. Do you have any type of cybersecurity in personal electronic devices?**

If yes:

- How many devices?
- What protection do you have? (e.g., anti-virus, security against phishing and dangerous websites, protection in e-commerce payments, etc.)
- [If you have minor children]: Are your children's devices also protected? If not, why do you think it is not necessary for your children?

If not

- What are the reasons inherent to your choice?
    - Lack of awareness (e.g. .: “We never thought about it”)
    - Lack of knowledge about the offer (e.g., “We would like to have cybersecurity, but we do not know how to obtain information about the offers on the market.”).
    - Lack of need (e.g., “The company does not have many risks” “The level of cybersecurity protects us in full against any possibility of loss.”, Etc.).
    - Inaccessible prices.

**4. Do you have cyber risk insurance?**

If yes:

- Is it independent insurance or is it included in a multi-risk?
- What is the insurance coverage?
- What were the criteria for choosing insurance?
    - Price;
    - Coverages;
    - Brand confidence;

# APPENDIX 9 – IN-DEPTH INTERVIEW GUIDE (B2C SEGMENT) – III/III

Back to Presentation

- How did you purchase this insurance?
  - Was it approached by a mediator? If so, do you consider the advice of your agent/mediator to have a significant bearing on your decision?
  - Did you find out at a counter?
  - Did you find out on the insurer's online channels?
- Did you have to fill out an initial form?

If not

- What are the reasons for this decision?
- Lack of awareness (e.g., “We never thought about it”)
- Lack of knowledge about the offer (e.g., “We would like to have cybersecurity, but we do not know how to obtain information about the offers on the market.”).
- Lack of need (e.g., “The company does not have many risks” “The level of cybersecurity protects us in full against any possibility of loss.”, Etc.). Because?
- Inaccessible prices.
- Have you considered the purchase? If so, what is the reason for not continuing?

**5. In recent times, have the words “cybersecurity”, “cyber attack”, “cyber risks”, “cybercrimes” come up more often in your life?**

- If so, in what contexts and why? (i.e., + frequency, + severity or both).

**6. Do you think you may be able to buy cyber risk insurance in the near future?**

If yes:

- What are the main coverages you would be looking for?
- Would you like it through the mediator/agent, counter, online?
- What monthly premium would they be willing to pay? Why?

7. Considers that the theft of your personal data (documents, photographs, private information) would have an impact similar to the theft of your assets with sentimental value (e.g., inherited objects).

## Agenda

## Survey to SMEs: Questions (I/XII)

### Cybersecurity Market Research

Objective: This questionnaire aims to collect data on the level of awareness, preparation, needs and preferences of small and medium-sized companies in relation to cybersecurity services, namely Insurance against cyber risks. Not being mandatory, we recommend that the questionnaire, when possible, be completed by an IT department employee or similar.

Requirement 1 (number of employees): maximum limit of 250.
Requirement 2 (turnover): maximum limit of 50 million euros.

Duration: The questionnaire lasts an average of 10 minutes.

Anonymity: Your responses are anonymous. We will analyze and publish the data in aggregate.

If you have any questions or comments about this questionnaire, please contact:

Afonso Gomes 29032@novasbe.pt Madalena Sangalho 29203@novasbe.pt Raquel Santos Brites 29212@novasbe.pt
Thank you very much in advance for your contribution!

**General information**

1

Industry in which the company operates: *

- Public administration
- Administrative
- Agriculture, animal production, hunting, forestry and fishing
- Accommodation and Food
- Arts, Entertainment and Recreation
- Real Estate Activities
- Wholesale Trade
- Retail Trade
- Education
- Energy and Utilities
- Engineering and Civil Construction
- Extractive Industry
- Manufacturing Industry
- Health and Social Assistance
- Financial services
- Management Services
- Professional, Scientific and Technical Services
- Information systems
- Transport and Storage
- Other

2

What is your company's annual turnover value? *

- Less than 1 million euros
- From 1 to 2 million euros
- From 2 to 3.50 million euros
- From 3.50 to 11 million euros
- From 11 to 18 million euros
- From 18 to 50 million euros
- More than 50 million euros

Following

## Survey to SMEs: Questions (II/XII)

More than 50 million euros

3

What is the number of employees in your company? *

- Less than 10
- Between 10 and 250
- More than 250

Following

These contents are created by the owner of the form. The data you submit will be sent to the owner of the form. Microsoft is not responsible for the privacy or security practices of its customers, including those of the owner of this form. Never

4

How dependent is the organization's operations on connected assets (IT and TO)?
(1 - Independent; 10 - Totally Dependent) *

1 2 3 4 5 6 7 8 9 10

5

What digital platforms are used by the company? *

- E-commerce (online sales)
- Marketplace
- Social networks
- Website

- Other

6

Does the company's organizational structure include different departments and IT managers?
(Select the options that apply) *

- IT department
- IT Security Area
- Chief Information Security Officer (CISO)
- Data Protection Officer (DPO)
- Does not include

7

By what regulation (s) / standard (s) is the company covered?
(Select the options that apply) *

- PCI-DSS
- ISO 27001
- RGPD
- NIS Directive
- Industry-specific regulations
- Other regulations
- Do not know

8

What is your position in the company?

Enter your answer

Section 1

9

Which of these cyber incidents are you familiar with?
(Select the options that apply) *

- Denial of Service (DDoS)
- Hacking
- Malware
- Ransomware
- Scamming
- Social Engineering (Phishing)
- Trojan
- Virus

**Note:** The answers to questions 2 and 3 were used to exclude micro and large companies.

## Survey to SMEs: Questions (III/XII)

Victims of a cyber incident

☐ Do not know

☐ Other

10

What are the consequences of cyber incidents that you consider most worrying for the organization? (Order from highest to lowest level of concern) *

- Compliance and litigation costs (eg fines, notification costs, etc.)
- Reputational damage
- Business interruption
- Loss and recovery of assets
- Drop in productivity and employee motivation (due to emotional / psychological distress)

11

Do you remember a recent cyber attack on a Portuguese company? *

◯ Yes

◯ Not

12

Which?

Enter your answer

Previous | Following

Section 2

13

Has the organization ever been the victim of a cyber incident? *

◯ Yes

◯ Not

14

How many times in the past 5 years? *

◯ 1 time

◯ 2-3 times

◯ 4 times or more

15

What type (s) of cyber incident (s) has the organization already been a victim of? (Select the options that apply) *

☐ Denial of Service (DDoS)

☐ Hacking

☐ Malware

☐ Ransomware

☐ Scamming

☐ Social Engineering (Phishing)

☐ Trojan

☐ Virus

☐ Do not know

☐ Other

16

What is the main motivation behind the cyber incident? (Select the options that apply) *

◯ Cyber espionage (the act of obtaining secrets and information without the permission of the holder for the personal advantage of the attacker)

◯ Cyber extortion (act of coercing the victim to pay a ransom in order to regain control of the information / systems)

◯ Hacktivism (act of intercepting information systems for political or ideological reasons)

◯ Do not know

**Notes:** Question 12 was only showed to those who answered "Yes" to question 11; Questions 14-20 were only showed to those who answered "Yes" to question 13 (i.e. victims of a cyber incident).

## Survey to SMEs: Questions (IV/XII)

| Victims of a cyber incident | Non-victims of a cyber incident |
|---|---|

Other

17
Assess the impact of each of the consequences of the cyber incident (s) in question?
(0 - There was no impact; 5 - High impact) *

Loss of assets

0
1
2
two
3
4
5

Business interruption

0
1
2
two
3
4
5

Reputational damage

Compliance and litigation costs

Drop in productivity and employee motivation (due to emotional / psychological distress)

18
To whom was the cyber incident (s) reported?
(Select the options that apply) *

Internal reporting

Reporting to authorities

Do not know

Other

19
How was the situation managed?
(Select the options that apply) *

Internally managed

Support from partners specialized in cybersecurity

Hiring cybersecurity services

Do not know

Other

20
Assess the impact of the cyber incident (s) on the company's perspective in relation to cybersecurity concerns?
(1 - There was no impact; 10 - High impact) *

2

1 two 3 4 5 6 7 8 9 10

Previous Following

14
What level of threat does your company face in relation to a potential attack?
(1 - No threat; 10 - Imminent threat)
*

2

1 two 3 4 5 6 7 8 9 10

15
If you assessed your threat level to be 5 or higher in the previous question: what / what are the inherent reason (s)?
(Select the options that apply)

Low level of cybersecurity

Company size

Sensitive and high value information

**Notes:** Questions 14-16 were only showed to those who answered “Not” to question 13 (i.e. non-victims of a cyber incident) on the previous slide.

## Survey to SMEs: Questions (V/XII)

### Non-victims of a cyber incident

- [ ] Company size
- [ ] Sensitive and high value information
- [ ] High brand image value
- [ ] Do not know
- [ ] Other

Previous | Following



Section 3

16

Assess the company's cybersecurity level.
(1 - Very low; 10 - Very high)

2

1 two 3 4 5 6 7 8 9 10

17

What are the cyber risk assessment measures adopted by the company?
(Select the options that apply) *

- [ ] Vulnerability analysis
- [ ] Verification of compliance with information security regulations / standards (eg GDPR, PCI-DSS, etc.)
- [ ] Security tests (eg intrusion tests, social engineering, red team assessment, etc.)
- [ ] None
- [ ] Do not know
- [ ] Other

18

What prevention / protection measures are adopted by the company?
(Select the options that apply) *

- [ ] Strong password policy
- [ ] Software update (including operating systems)
- [ ] User identification and multi-factor authentication
- [ ] Encryption techniques for data, emails and documents
- [ ] Network access control (management of access by devices and users to the company network)
- [ ] VPN (extends a private network to allow secure exchange of data over the public network)
- [ ] Awareness / training of employees
- [ ] Backup data to a separate location (including cloud backup)
- [ ] None
- [ ] Do not know
- [ ] Other

19

What are the contingency rules adopted by the company?
(Select the options that apply) *

- [ ] Incident response plans
- [ ] Cyber risk monitoring
- [ ] Periodic review and update of cybersecurity measures
- [ ] None
- [ ] Do not know
- [ ] Other

20

Who applies and monitors cybersecurity measures? *

## Survey to SMEs: Questions (VI/XII)

**20**

Who applies and monitors cybersecurity measures? *

- ○ Company (internally)
- ○ External suppliers
- ○ Mixed (company and external suppliers)
- ○ Do not know

Previous | Following



**21**

What type (s) of external supplier (s)? (Select the options that apply) *

- ☐ Cybersecurity supplier
- ☐ Cybersecurity consultants / auditors
- ☐ Insurer with cyber risk insurance
- ☐ Do not know
- ☐ Other

Previous | Following

**Section 4**

**22**

Does the company have insurance against cyber risks? *

- ○ Yes, independent insurance
- ○ Yes, included in multi-risk insurance
- ○ Not

Previous | Following

### Companies with cyber insurance

**23**

What motivated the company to buy insurance against cyber risks? (Select the options that apply) *

- ☐ Low level of cybersecurity
- ☐ Company size
- ☐ High brand image value
- ☐ Occurrence of a cyber incident
- ☐ Sensitive and high value information
- ☐ Digital transformation
- ☐ Do not know
- ☐ Other

**24**

What risk mitigation services are included in the insurance? (Select the options that apply) *

- ☐ Vulnerability analysis
- ☐ Assessment of compliance with information security regulations / standards (eg GDPR, PCI DSS, ISO 27001, etc.)
- ☐ Intrusion tests
- ☐ Hardening
- ☐ Red Team Review
- ☐ Social engineering
- ☐ Data backup
- ☐ Training of employees

**Notes:** Question 21 is only showed to those who answered “external suppliers” or “mixed (company and external suppliers); Questions 23-33 were only showed to those who answered ”Yes, independent insurance” or “Yes, included in multi-risk insurance” in question 22 (i.e. companies with cyber insurance).

## Survey to SMEs: Questions (VII/XII)

### Companies with cyber insurance

- ☐ Periodic monitoring of cyber risks
- ☐ Incident response plan
- ☐ Do not know
- ☐ none
- ☐ Other

25
What coverages are included in cyber risk insurance?
(Select the options that apply) *

- ☐ Fraud / theft costs
- ☐ Costs of loss and recovery of computational assets (infrastructure and information)
- ☐ Forensic costs (eg court costs, compensation for breach of privacy / confidentiality, litigation costs)
- ☐ Business Interruption Costs
- ☐ Do not know
- ☐ Nennhuma
- ☐ Other

26
What post-accident assistance services are included in cyber risk insurance?
(Select the options that apply) *

- ☐ Technical support (restoration of computational assets - infrastructure and information)
- ☐ IT forensic investigation
- ☐ Legal advice and legal aid
- ☐ Notification and communication
- ☐ Public relations and crisis management
- ☐ Do not know
- ☐ none
- ☐ Other

27
How did you purchase the insurance?
(Select the options that apply) *

- ☐ The company was approached by a mediator
- ☐ The company contacted a mediator
- ☐ The company was informed of the offer (s) through the online channels of the insurance companies
- ☐ Do not know
- ☐ Other

28
Evaluate your experience in completing the membership form, in the following areas:
(0 - Not satisfied; 5 - Totally satisfied)
*

Extension

- ○ 0
- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ Do not know

Language

29
Would the company be willing to pay a fee to enjoy personalized support in filling out the membership form? *

- ○ Yes
- ○ Not

# APPENDIX 10 – SURVEYS: QUESTIONS

## Survey to SMEs: Questions (VIII/XII)

### Companies with cyber insurance

Do not know

30

Did you have access to an online tool for preliminary assessment of the company's level of exposure to cyber risks (as shown in the image)? *


Yes

Not

Do not know

Picture of risk assessment too in slide z

31

What are the most relevant criteria when selecting insurance against cyber risks?
(Order from most to least relevant) *

- Accessibility of the membership form
- Coverings
- Trust in the insurer or mediator
- Price
- Additional services (prevention, protection and assistance)

32

What is the annual premium that the

What is the annual premium that the company pays for insurance against cyber risks? *

- Less than 750 euros
- From 750 to 1500 euros
- From 1500 to 3 thousand euros
- From 3 thousand to 6 thousand euros
- From 6 thousand to 12 thousand euros
- More than 12 thousand euros
- Do not know

33

How satisfied is the company with cyber risk insurance? *

33

How satisfied is the company with cyber risk insurance? *

- Not satisfied
- Not very satisfied
- Satisfied
- Very satisfied

Previous | Following

These contents are created by the owner of the form. The data you submit will be sent to the owner of the form. Microsoft is not responsible for the privacy or security practices of its

### Companies without cyber insurance

23

Why has the organization not yet purchased cyber risk insurance? (Select the options that apply) *

- I was not aware of the existence of this insurance
- The company's level of cybersecurity is sufficient
- Inaccessible prices
- Complex membership form
- Restricted coverage
- Other

24

Can cybersecurity gain relevance at the top of your company's priorities? *

**Notes:** Questions 23-33 were only showed to those who answered ”Not” in question 22 (i.e. companies without cyber insurance).

## Survey to SMEs: Questions (IX/XII)

### Companies without cyber insurance

23

Why has the organization not yet purchased cyber risk insurance? (Select the options that apply) *

- I was not aware of the existence of this insurance
- The company's level of cybersecurity is sufficient
- Inaccessible prices
- Complex membership form
- Restricted coverage
- Other

24

Can cybersecurity gain relevance at the top of your company's priorities? *

29

Can cybersecurity gain relevance at the top of your company's priorities? *

- Yes
- Perhaps
- Not

30

Why do you think you can gain relevance at the top of the company's priorities? *

- Regulations and standards (eg GDPR, PCI-DSS, etc.)
- Increased cyber attacks
- Increased remote work
- Other

31

What is the company's willingness to purchase insurance against cyber risks that would cover all the needs of the organization in the next 2 years? *

- No provision
- Any provision
- High layout
- Total provision

Previous | Following

32

What are the main features that you would be looking for when buying insurance against cyber risks? (0 - Irrelevant; 5 - Totally relevant) *

Vulnerability analysis

- 0
- 1
- 2
- 3
- 4
- 5
- Do not know

Assessment of compliance with information security regulations / standards

Intrusion tests

Hardening

Red Team Review

Social Engineering Tests

Data backup

Training for employees

Fraud / theft costs

Costs of loss / recovery of computational assets

**Note:** Question 32 was only showed to those who did not answer ”No provision” in question 31.

## Survey to SMEs: Questions (X/XII)

### Companies without cyber insurance

- Business interruption costs
- Forensic costs
- Technical support
- IT forensic investigation
- Legal advice and legal sponsorship
- Notification and communication
- Public relations and crisis management
- Periodic monitoring of cyber risks
- Incident response plan

33

How would you like to purchase this insurance?
(Select the options that apply) *

- ☐ Website
- ☐ General Mediator
- ☐ Cyber risk insurance mediator
- ☐ Other

34

How relevant would it be to have access to an online tool for preliminary assessment of the company's level of exposure to cyber risks (as shown in the image), before purchasing insurance?
(1- Irrelevant, 5 - Very relevant) *


1 2 3 4 5

35

What annual premium would the organization be willing to pay for cyber risk insurance? *

- Less than 750 euros
- From 750 to 1500 euros
- From 1500 to 3 thousand euros
- From 3 thousand to 6 thousand euros
- From 6 thousand to 12 thousand euros
- More than 12 thousand euros

Previous | Following

These contents are created by the owner of the form. The data you submit will be sent to the owner of the form. Microsoft is not responsible for the privacy or security practices of its customers, including those of the owner of this form. Never reveal your password.

Powered by Microsoft Forms | Privacy and Cookies| Terms of Use

#### Awareness

Below we present a video with some of the main data related to cyber incidents in SMEs. After viewing the video, we would like you to answer the last 4 questions.


Picture of risk assessment tool in slide 153

## Survey to SMEs: Questions (XI/XII)

39

Assess the company's cybersecurity level.
(1 - Very low; 10 - Very high) *

1 2 3 4 5 6 7 8 9 10

40

Would the company be willing to replace current insurance with an offering that would cover all of the organization's cybersecurity needs? *

- Yes
- Perhaps
- Not

41

What are the main features you would be looking for in the new cyber insurance?
(0 - Irrelevant; 5 - Totally relevant) *

Vulnerability analysis

- 0
- 1
- 2
- 3
- 4
- 5
- Do not know

Assessment of compliance with information security regulations / standards

Red Team Review

Hardening

Intrusion tests

Social engineering

Data backup

Training for employees

Fraud / theft costs

Costs of loss / recovery of computational assets

Business interruption costs

Forensic costs

Technical support

IT forensic investigation

Legal advice and legal sponsorship

Notification and communication

Public relations and crisis management

Periodic monitoring of cyber risks

Incident response plan

Online cyber risk assessment tool

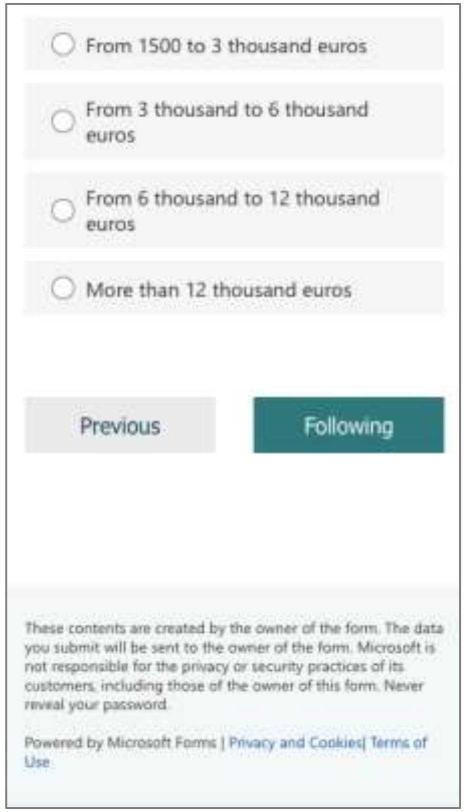
42

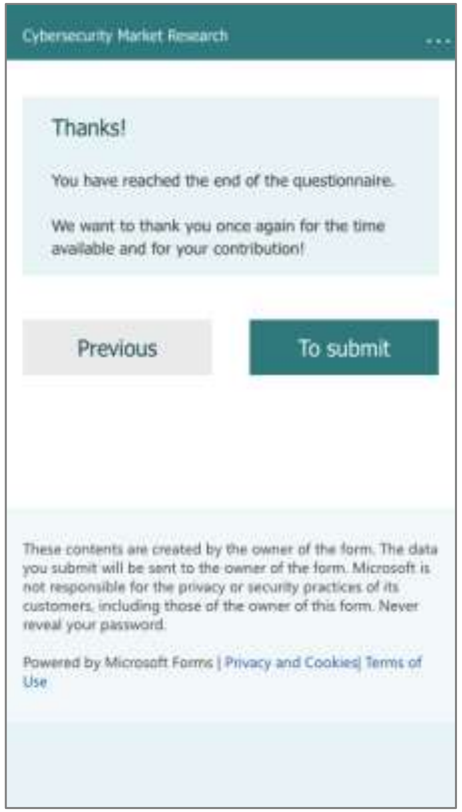
How much would the company be willing to pay for the new cyber risk insurance that would cover all the organization's needs? *

- Less than 750 euros
- From 750 to 1500 euros
- From 1500 to 3 thousand euros
- From 3 thousand to 6 thousand euros
- From 6 thousand to 12 thousand euros
- More than 12 thousand euros

**Notes:** Questions 40 and 41 are only showed to the companies with cyber insurance. Companies without cyber insurance have a similar question to no. 40 with the substitution of the word “replace” to “buy”.

## Survey to SMEs: Questions (XII/XII)




## Survey to Individuals: Questions (I/XIII)

### Cybersecurity Market Study

Objective: This questionnaire aims to collect data on the level of awareness, preparation, needs and preferences of consumers in relation to cybersecurity services, namely Insurance against cyber risks.

Duration: The questionnaire lasts an average of 10 minutes.

Anonymity: Your responses are anonymous. We will analyze and publish the data in aggregate.

If you have any questions or comments about this questionnaire, please contact:

Afonso Gomes 29032@novasbe.pt Madalena Sangalho 29203@novasbe.pt Raquel Santos Brites 29212@novasbe.pt
Thank you very much for your contribution!

* Required

* Required

1
Age *

- Less than 18
- 18 - 29
- 30 - 39
- 40 - 49
- 50 - 59
- 60 - 65
- More than 65

2
Assess the level of dependence on your daily activities (leisure, shopping and financial operations) on the internet?
(1 - Totally independent - does not use internet; 10 - Totally dependent - uses internet in all daily activities) *

1 two 3 4 5 6 7 8 9 10

3
Do you carry out financial transactions over the internet (eg homebanking, online shopping, etc.)? *

- Yes
- Not

4
What financial transactions do you most frequently do online?
(0 - I do not do it; 5 - I do it daily) *

E-commerce (purchases of goods or services online)

- 0
- 1
- two
- 3
- 4
- 5

Homebanking (Online banking)

5
Are you subscribed to any social network? *

- Yes
- Not

Following

These contents are created by the owner of the form. The data you submit will be sent to the owner of the form. Microsoft is not responsible for the privacy or security practices of its customers, including those of the owner of this form. Never reveal your password.

Powered by Microsoft Forms | Privacy and Cookies| Terms of Use

## Survey to Individuals: Questions (II/XIII)

6

Which social networks do you use most often?
(0 - I don't use it; 5 - I use it daily) *

Facebook

- 0
- 1
- two
- 3
- 4
- 5

Instagram

LinkedIn

7

How often do you share personal content (eg family photos, frequent places) on your social networks? *

- Daily
- Weekly
- 2-3 times a month
- Monthly
- Less than once a month
- Never

8

How private are your social media accounts? *

8

How private are your social media accounts? *

- Private, close friends only
- Private, known
- Public

9

Through what medium (s) do you store and / or share your electronic files (eg documents, photos and / or videos, personally identifiable data, etc.)?
(Select the options that apply) *

- Social networks
- E-mails with attached files

9

Through what medium (s) do you store and / or share your electronic files (eg documents, photos and / or videos, personally identifiable data, etc.)?
(Select the options that apply) *

- Social networks
- E-mails with attached files
- Clouds
- I don't share or store files online
- Other

10

What type (s) of online risk behavior (s) do you identify with?
(Select the options that apply) *

10

What type (s) of online risk behavior (s) do you identify with?
(Select the options that apply) *

- Install unauthorized apps / programs
- Browse unprotected sites (unauthorized platforms for games, movies, series, etc.)
- Turn off automated security tools
- Participate in "chat rooms"
- none

11

Taking into account your level of exposure and dependence on electronic devices, what is the level of threat you face in relation to a

# APPENDIX 10 – SURVEYS: QUESTIONS

## Survey to Individuals: Questions (III/XIII)

11

Taking into account your level of exposure and dependence on electronic devices, what is the level of threat you face in relation to a possible cyber attack?
(1 - No threat; 10 - Imminent threat)
*

1 two 3 4 5 6 7 8 9 10

12

If you assessed your threat level to be 5 or higher in the previous question: what is the reason (s) inherent in that threat level?

- Low level of cybersecurity
- High media exposure
- Relevant position in the

12

If you assessed your threat level to be 5 or higher in the previous question: what is the reason (s) inherent in that threat level?

- Low level of cybersecurity
- High media exposure
- Relevant position in the organization where you work
- Other

13

If in the previous question you considered "high media exposure" as an inherent reason, please indicate the type (s) of media exposure.

- Artist (TV, music)

13

If in the previous question you considered "high media exposure" as an inherent reason, please indicate the type (s) of media exposure.

- Artist (TV, music)
- High competition athlete
- Content creator
- Political
- Other

Following

Cybersecurity Market Study ...

* Required

Section 2

14

Have you ever been the victim of a cyber attack? *

- Yes
- Not

Previous Following

These contents are created by the owner of the form. The data

15

Do you know anyone who has been the victim of a cyber attack? *

- Yes
- Not

Previous Following

These contents are created by the owner of the form. The data you submit will be sent to the owner of the form. Microsoft is not responsible for the privacy or security practices of its customers, including those of the owner of this form. Never reveal your password.

Powered by Microsoft Forms | Privacy and Cookies| Terms of Use

## Survey to Individuals: Questions (IV/XIII)

**Victims or know a victim of cyber crime**

15

How many times in the past 5 years? *

- 1
- two
- 3 or more

16

What type (s) of cyber attack (s) did you fall victim to?
(Select the options that apply) *

- Hacking (access to computers / networks through breaches of security measures)
- Malware (malicious program or code harmful to computer systems)

16

What type (s) of cyber attack (s) did you fall victim to?
(Select the options that apply) *

- Hacking (access to computers / networks through breaches of security measures)
- Malware (malicious program or code harmful to computer systems)
- Ransomware (act of coercing the victim to pay a repair in order to regain control of the information / systems)
- Social Engineering (manipulation of electronic communication to assume the identity of a trusted person / organization, in order to access confidential user information)
- Trojan (malware that enters the device as a common and

17

What is the purpose (s) of the cyber attack (s)?
(Select the options that apply) *

- Illegal access to bank credentials
- Identity theft
- Virtual harassment (eg cyberbullying)
- Illegal access to documents / personal data (photos, videos, etc.)
- Do not know
- Other

18

Assess the impact of each of the

18

Assess the impact of each of the consequences of the cyber incident (s) in question?
(0 - There was no impact; 5 - High impact) *

- Financial consequences
- Psychological or emotional consequences
- Reputational consequences
- Waste of time in resolving the incident

19

Who did you report the incident to?
(Select the options that apply) *

19

Who did you report the incident to?
(Select the options that apply) *

- Authorities (PJ, PSP, GNR, etc.)
- Portuguese Victim Support Association (APAV)
- Digital platform in question (ex: social network, website, app, etc.)
- Not reported
- Do not know

Previous | Following

## Survey to Individuals: Questions (V/XIII)

**Non-victims**

12
What are the objectives of a potential cyber incident that you consider most worrying?
(Order from highest to lowest level of concern) *

- Illegal access to bank credentials
- Identity theft
- Virtual harassment (eg cyberbullying)
- Illegal access to documents / personal data (photos, videos, etc.)

13
What are the consequences of a potential cyber incident that you find

13
What are the consequences of a potential cyber incident that you find most worrying?
(Order from highest to lowest level of concern) *

- Financial consequences
- Emotional / psychological consequences
- Reputational consequences
- Waste of time in resolving the incident

Previous | Following

Cybersecurity Market Study ...

* Required

20
Do you have minor children? *

- Yes
- Not

Previous | Following

These contents are created by the owner of the form. The data you submit will be sent to the owner of the form. Microsoft is not responsible for the privacy or security practices of its customers, including those of the owner of this form. Never reveal your password.

**Parents only**

21
Has your child (ren) ever been a victim of cyberbullying? *

- Yes
- Not
- Do not know

Previous | Following

These contents are created by the owner of the form. The data you submit will be sent to the owner of the form. Microsoft is not responsible for the privacy or security practices of its customers, including those of the owner of this form. Never reveal your password.

22
How serious are cyberbullying episodes?
(1 - Very Slight; 5 - Very Severe) *

1 | two | 3 | 4 | 5

23
What is the relationship between the attacker and the victim of cyberbullying? *

- Schoolmate
- Friend
- Family
- Unknown
- Do not know

## Survey to Individuals: Questions (VI/XIII)

**Parents only**

24

What is the level of concern about cyberbullying in your household?
(1 - No concern; 10 - Total concern) *

| 1 | two | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

Previous | Following

These contents are created by the owner of the form. The data you submit will be sent to the owner of the form. Microsoft is not responsible for the privacy or security practices of its customers, including those of the owner of this form. Never reveal your password.

Powered by Microsoft Forms | Privacy and Cookies| Terms of Use

19

What type (s) of online security measure (s) do you identify with?
(Select the options that apply) *

- ☐ Use different emails for different accounts
- ☐ Use strong and different passwords
- ☐ Clear your browser's cache (search engine)
- ☐ Disable the "save password" feature
- ☐ Update software and operating systems
- ☐ None of the above

**Parents only**

22

Do you monitor your children's online activity? *

- ○ Yes
- ○ Not

Previous | Following

These contents are created by the owner of the form. The data you submit will be sent to the owner of the form. Microsoft is not responsible for the privacy or security practices of its customers, including those of the owner of this form. Never reveal your password.

Powered by Microsoft Forms | Privacy and Cookies| Terms of Use

23

Monitor your children's online activity by what means?
(Select the options that apply) *

- ☐ Parental control apps or software (eg Bark, Qustodio, Net Nanny, Kaspersky Safe Kids, etc.)
- ☐ I monitor your activities on online platforms (ex: social networks, games, etc.)
- ☐ Internet access time limits
- ☐ Other

24

Do you have any type of protection against cyber attacks on your personal electronic devices (eg mobile phone, computer, tablet, etc.)? *

24

Do you have any type of protection against cyber attacks on your personal electronic devices (eg mobile phone, computer, tablet, etc.)? *

- ○ Yes, free of charge
- ○ Yes, through a paid product / service
- ○ Not
- ○ Do not know

Previous | Following

## Survey to Individuals: Questions (VII/XIII)

25

What type (s) of protection?
(Select the options that apply) *

- Anti-virus
- Multi-factor authentication
- Encryption techniques for data, emails and documents
- VPN (extends a private network to allow secure exchange of data over the public network)
- Backup data to a separate location (including cloud backup)
- Other

26

Compared to the protection of your

**Parents only**

26

Compared to the protection of your electronic devices, what is the protection existing in the devices used by your child (ren)? *

- Protection level higher than mine
- Same level of protection
- Protection level lower than mine
- Do not know

Previous | Following

Cybersecurity Market Study

* Required

28

Do you have insurance against cyber risks? *

- Yes
- Not

Previous | Following

These contents are created by the owner of the form. The data you submit will be sent to the owner of the form. Microsoft is not responsible for the privacy or security practices of its customers, including those of the owner of this form. Never

**People with cyber insurance**

29

What are the characteristics of insurance against cyber risks that you have?
(Select the options that apply) *

- Family insurance
- Personal insurance
- Independent insurance
- Insurance included in multi-risk insurance
- Pre-defined coverages
- Ability to modularly choose covers
- Do not know

30

30

What motivated you to purchase insurance against cyber risks?
(Select the options that apply) *

- Low level of cybersecurity
- Relevant position in the organization where you work
- High media exposure
- Concern for my children's safety
- Do not know
- Other

31

What protection services are included in cyber risk insurance?
(Select the options that apply) *

**Notes:** in question 30 for non-parents there is no option "growing concern about my children's online safety".

## Survey to Individuals: Questions (VIII/XIII)

### People with cyber insurance

31

What protection services are included in cyber risk insurance?
(Select the options that apply) *

- Anti-virus
- Firewalls
- Multi-factor authentication
- Backup data to a separate location (including cloud backup)
- VPN (extends a private network to allow secure exchange of data over the public network)
- Encryption techniques for data, emails and documents
- Online parental control software
- none

32

What coverages are included in cyber risk insurance?
(Select the options that apply) *

- Theft / fraud costs
- Costs of loss / recovery of computational assets (devices and data)
- Forensic costs
- None
- Do not know
- Other

33

What assistance services are included in cyber risk insurance?
(Select the options that apply) *

33

What assistance services are included in cyber risk insurance?
(Select the options that apply) *

- Technical support (restoration of computational assets - infrastructure and information)
- Legal advice and legal sponsorship
- Psychological counseling (for children / young people who are victims of cyberbullying)
- Public relations
- None
- Do not know
- Other

34

How did you purchase the insurance?
(Select the options that apply) *

- I was approached by a mediator
- I contacted a mediator
- I learned about the offer (s) through the online channels of the insurance companies
- I was informed of the offer (s) in physical stores
- I learned about the offer (s) through the telephone contact
- Do not know
- Other

35

35

What are the most relevant criteria when selecting insurance against cyber risks?
(Order from most to least relevant) *

- Coverings
- Trust in the insurer or mediator
- Price
- Additional services (post-accident protection and assistance)

36

What is the annual premium you pay for insurance against cyber risks? *

**Notes:** Question 31: for non-parents there is no option “online parental control software”; question 33: for non-parents there is no option “psychological counselling”

## Survey to Individuals: Questions (IX/XIII)

### People with cyber insurance

36
What is the annual premium you pay for insurance against cyber risks? *

- Less than € 40
- Between 40 € and 60 €
- Between 60 € and 80 €
- Between 80 € and 100 €
- More than 100 €

37
How satisfied are you with cyber risk insurance? *

- Not at all satisfied

37
How satisfied are you with cyber risk insurance? *

- Not at all satisfied
- Not very satisfied
- Satisfied
- Very satisfied

Previous | Following

These contents are created by the owner of the form. The data you submit will be sent to the owner of the form. Microsoft is not responsible for the privacy or security practices of its customers, including those of the owner of this form. Never

### People without cyber insurance

29
Why have you not yet purchased cyber risk insurance?
(Select the options that apply) *

- I was not aware of the existence of this insurance
- The level of cybersecurity I have is sufficient
- Inaccessible prices
- Restricted coverage
- Other

30
Can cybersecurity gain relevance at the top of your priorities? *

33
Can cybersecurity gain relevance at the top of your priorities? *

- Yes
- Perhaps
- Not

Previous | Following

These contents are created by the owner of the form. The data you submit will be sent to the owner of the form. Microsoft is not responsible for the privacy or security practices of its customers, including those of the owner of this form. Never reveal your password.

Powered by Microsoft Forms | Privacy and Cookies| Terms of

34
Why do you think you can gain relevance at the top of your priorities?
(Select the options that apply) *

- Increased cyber attacks
- Increased remote work
- Growing concern about my children's online safety
- Do not know
- Other

35
What is your willingness to purchase insurance against cyber risks that would cover all your needs in the next 2 years? *

**Notes:** in question 34 for non-parents there is no option “growing concern about my children’s online safety”.

## Survey to Individuals: Questions (X/XIII)

People without cyber insurance

35

What is your willingness to purchase insurance against cyber risks that would cover all your needs in the next 2 years? *

- No provision
- Any provision
- High layout
- Total provision

Previous | Following

36

What insurance would you prefer to purchase? *

- Individual
- Family

37

Which insurance structure would you prefer to purchase? *

- Independent cyber risk insurance
- Cyber risk insurance included in a multi-risk

38

What are the main features that you

38

What are the main features that you would be looking for when buying insurance against cyber risks?
(0 - Irrelevant; 5 - Totally relevant) *

- Antivirus
- Firewalls
- Multi-factor authentication
- Backup data to a separate location
- VPN
- Data, document and email encryption techniques
- Online parental control software
- Online parental control software
- Theft / fraud cost
- Cost of loss / recovery of computational assets
- Forensic costs
- Technical support
- Legal advice and legal sponsorship
- Psychological counseling (of child / youth cyber bullying)

39

How would you like to purchase this insurance?

39

How would you like to purchase this insurance?
(Select the options that apply) *

- Online channels (ex: website)
- Mediator
- Contact by phone / email
- Physical store
- Other

40

What annual premium would you be willing to pay for cyber risk insurance? *

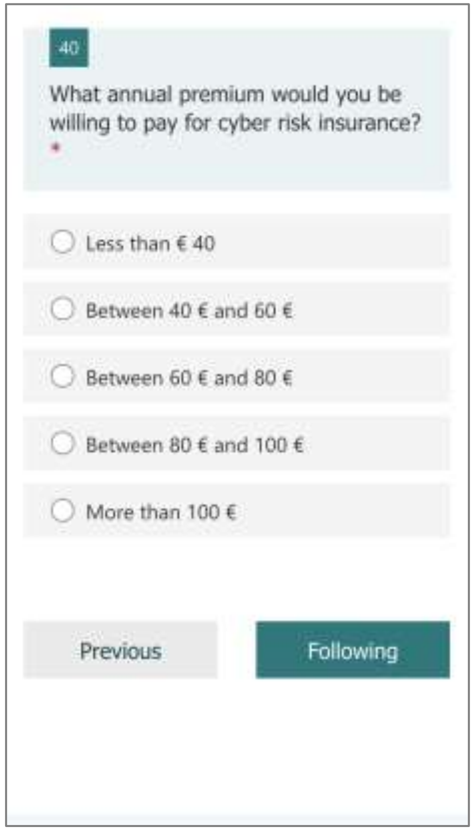
- Less than € 40

Only people with, at least any provision to buy insurance

**Notes:** in question 38 for non-parents there is no option "online parental control software" or "psychological counselling".

## Survey to Individuals: Questions (XI/XIII)

People without cyber insurance


40

What annual premium would you be willing to pay for cyber risk insurance? *

- Less than € 40
- Between 40 € and 60 €
- Between 60 € and 80 €
- Between 80 € and 100 €
- More than 100 €

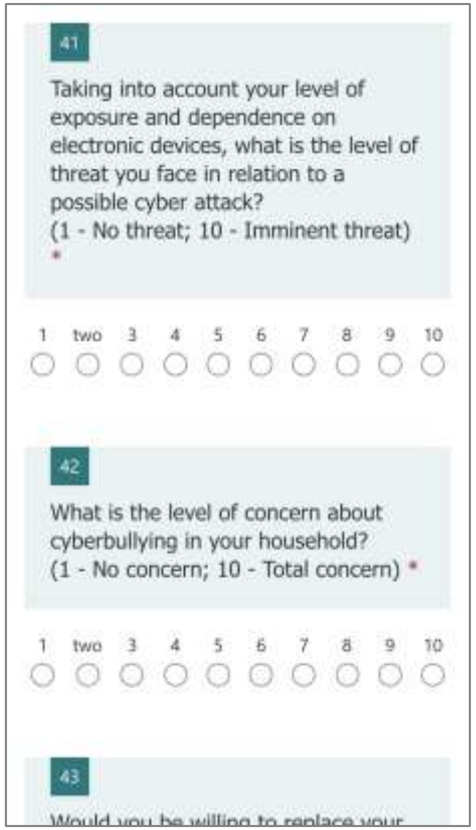
Previous | Following


Awareness

Below we present a video with some of the main data related to cyber attacks on the population. After viewing the video, we would like you to answer just five questions.



41


41

Taking into account your level of exposure and dependence on electronic devices, what is the level of threat you face in relation to a possible cyber attack?
(1 - No threat; 10 - Imminent threat) *

1 two 3 4 5 6 7 8 9 10

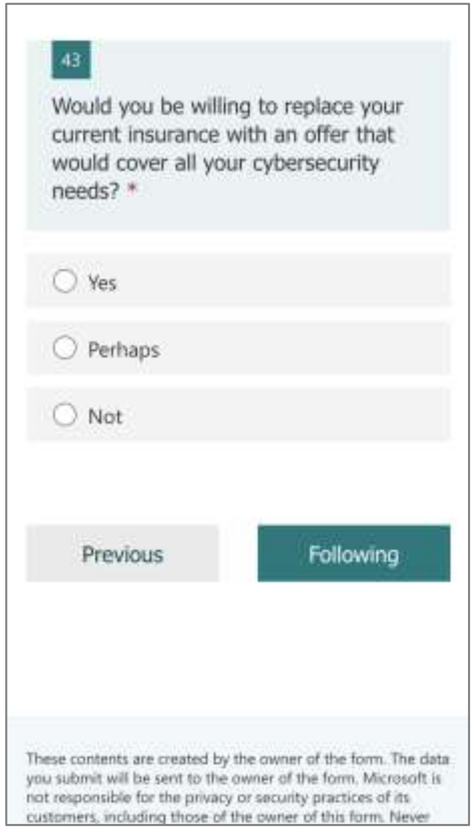
42

What is the level of concern about cyberbullying in your household?
(1 - No concern; 10 - Total concern) *

1 two 3 4 5 6 7 8 9 10

43

Would you be willing to replace your

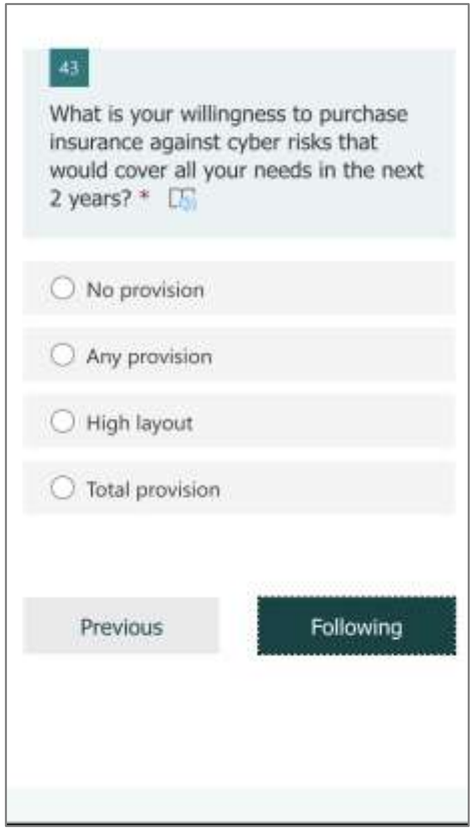

43

Would you be willing to replace your current insurance with an offer that would cover all your cybersecurity needs? *

- Yes
- Perhaps
- Not

Previous | Following

These contents are created by the owner of the form. The data you submit will be sent to the owner of the form. Microsoft is not responsible for the privacy or security practices of its customers, including those of the owner of this form. Never


43

What is your willingness to purchase insurance against cyber risks that would cover all your needs in the next 2 years? *

- No provision
- Any provision
- High layout
- Total provision

Previous | Following

Only people with, at least any provision to buy insurance

People with cyber insurance

People without cyber insurance

## Survey to Individuals: Questions (XII/XIII)

44

What are the main features you would be looking for in the new cyber risk insurance?
(0 - Irrelevant; 5 - Totally relevant) *

- Antivirus
- Firewalls
- Multi-factor authentication
- Backup data to a separate location
- VPN
- Data, document and email encryption techniques
- Online parental control software
- Theft / fraud cost
- Cost of loss / recovery of computational assets
- Forensic costs
- Technical support
- Legal advice and legal sponsorship
- Psychological counseling (of child / youth cyber bullying)

45

What annual premium would you be willing to pay for the new cyber risk insurance? *

45

What annual premium would you be willing to pay for the new cyber risk insurance? *

- Less than € 40
- Between 40 € and 60 €
- Between 60 € and 80 €
- Between 80 € and 100 €
- More than 100 €

Previous | Following

Cybersecurity Market Study

* Required

Personal information

46

Genre *

- Male
- Female
- Non-binary
- I prefer not to reveal

47

What is your area of residence? *

47

What is your area of residence? *

- North
- center
- Lisbon Metropolitan Area
- Alentejo
- Algarve
- Autonomous Region of the Azores
- Autonomous Region of Madeira

48

What is your occupation? *

People willing to replace or buy

People willing to replace or buy

**Notes:** in question 44 for non-parents there is no option "online parental control software".

Back to Presentation

## Survey to Individuals: Questions (XIII/XIII)

48

What is your occupation? *

- Student
- Student worker
- Self-employed
- Employee
- Unemployed
- Retired
- Other

49

What is the highest academic degree completed? *

- Basic education
- High school
- Professional course
- Graduation
- Postgraduate studies
- Master's
- Doctorate

50

How many people are in your household? *

- 1
- two
- 3-4
- 5 or more

51

What level of gross annual income does your household fall into? *

- Less than € 5,000
- Between € 5,001 to € 13,500
- Between € 13,501 to € 19,000
- Between € 19,001 to € 32,500
- Between € 32,501 to € 50,000
- Between € 50,001 to € 100,000
- Between € 100,001 to € 250,000
- More than € 250,000

Previous | Following

Cybersecurity Market Study

Thanks!

You have reached the end of the questionnaire.

We want to thank you once again for the time available and for your contribution!

Previous | To submit

## Agenda

# APPENDIX 11 – INDUSTRY EXPERTS INTERVIEWS (KEY INSIGHTS)

## Key Insights (I/II)

### IT Providers

*"The underlying logic is – after a phase where [cybersecurity] was not at all a concern – (…) we are now at a stage where the buzzword is* ***"Zero Trust"*** *and now the logic is to* ***draw*** *and* ***operate*** *everything considering that* ***anything can potentially be an attack****"*

*- Abel Aguiar*

### Other Industry Experts

Prof. Henrique Santos (UMinho)

Eng. José Galamba de Oliveira (APS)

Prof. Miguel Pardal (IST)

*"There is a* ***huge opportunity*** *for* ***cyber insurers*** *as they* ***take*** *the remaining* ***risk*** *that the organization does not want to take."*

*- Professor Henrique Santos*

### *Example: IDC – Digital Transformation Interview*

### IT Consulting Firms

*"Companies will want to* ***replace*** *the current multiple suppliers of cybersecurity products* ***with a single partner****. Thus, cybersecurity big players will need to* ***expand their offering portfolios*** *– establishing partnerships with service suppliers (including insurers). The* ***insurance industry*** *has a* ***whole range*** *of legal regulations, formalities, and procedures, unique to its activity that* ***tech companies*** *will* ***never*** *be able to* ***internalize****."*

*- Bruno Horta Soares (IDC)*

### Cybersecurity Providers

*"On a scale of* ***1*** *to* ***10*** *where 10 represents the maximum level of awareness,* ***large*** *companies score* ***6****, while* ***SMEs*** *and* ***individuals*** *score* ***3****."*

*- Rui Shantilal (Integrity)*

*"There are* ***no companies*** *that are* ***not attacked****. There are companies that know and others that* ***do not even know*** *they've been attacked."*

*- Vítor Rodrigues (S2 Group)*

*"As we, unfortunately, see the* ***growth*** *of* ***ferocious attacks*** *succeeding and the breach of private information, more and more* ***SMEs*** *will rely on* ***external cybersecurity services****, not least because they do* ***not have*** *the* ***capacity*** *to do so* ***internally****."*

*- António Ribeiro (Claranet)*

## Key Insights (II/II)

### Evolution of Cyber Crimes

**Shift** from technology-based attacks to social engineering:

| Technological | Social engineering |
|---|---|
| Vulnerability in the **virus**, **firewalls**, etc. – more expensive attacks | Vulnerability in the **human error** (e.g., clicking on links, opening fraudulent emails, etc.) – **more profitable attacks** |

### Cyber Awareness

**Increasing Cyber Awareness in Portuguese Companies**

- **An Increasing number of large-scale attacks** covered by the media (e.g., Ransomware attack in CUF; Football Leaks)
- **Creation of CNCS** (*Centro Nacional de Cibersegurança*) – promotion of activities and resources to increase awareness
- **Increasing automation of processes** provided by the 5G technology raises concerns, especially in OT security
- **Covid-19 pandemic** has increased cybersecurity measures in companies (especially large ones) in a very short period.

### Cybersecurity Level of Portuguese Companies

#### SME's

Most companies lack a comprehensive cybersecurity strategy and are **incapable of internalizing cybersecurity services**:

- **Lack of resources** – companies do not see cybersecurity as a priority until they suffer an attack.
- **Lack of IT Professionals** – most companies do not possess any IT representative – all dimensions of cybersecurity are outsourced

**Low Maturity**

#### Large Companies

**High commitment** to cybersecurity – most of these companies have Information Security Departments – the issue is no longer an IT-only but also a Board responsibility:

- **Banking** - most advanced technology in cybersecurity – due to increasing regulation (namely the PCI-DSS)
- **Utilities** - High investment in OT security in energy, oil, and gas companies

**High Maturity**

## Agenda

## B2B Segment – Key Insights (I/II)

### Healthcare and Social Assistance

**Clínica Europa – Grupo Joaquim Chaves**

*"**Healthcare** companies carry an **additional burden** when it comes to **data sensitivity**."*

*- Jorge Soares – IT Manager*

### Educational SERVICES

**IFA - Instituto de Formação Aeronáutica, Lda.**

*"[Cyber incidents] are a **daily reality** either in the emails we receive, on the websites we visit or in the messages we open on the phone. It's a reality and we have to **watch out for it**."*

*- Luís Giraldes – Marketing & Sales Manager*

### KEY INSIGHTS

#### Awareness

- **Phishing, ransomware, and malware** are the most frequently mentioned incidents;
- **Business interruption**, **reputational costs** and, **loss of information** are the major consequences identified;
- 2 out of 4 companies had already suffered a cyber incident

#### Level of Cybersecurity

- **Preventive measures:** most companies implemented a GDPR compliance plan;
- **Protective measures:** most companies have employee education, IT security systems, password policies, and regular back-up plans;
- **Contingency and monitoring plans:** 3 out of the 4 companies have a disaster recovery plan;
- **Vertical integration:** 3 out of the 4 companies have most pre-breach services internalized.

## B2B Segment – Key Insights (II/II)

### Professional, Scientific and Technical Services

**JcDecaux Portugal**

*"**Prevention** is the focal point of cybersecurity in any organization – it involves not only **technology** but also **training employees** for this topic"*

*- Rui Luís – IT Manager*

### Manufacturing

**Rozès, S.A.**

*"I have never considered acquiring **cyber risk insurance**, but nowadays it might start to **make sense**."*

*- Paulo Santos – Manager*

### KEY INSIGHTS

**Cyber Insurance**

- Only 1 out of the 4 companies has cyber insurance – the remaining companies identify **lack of necessity** and **awareness** as the main reasons for not having it;
- Cyber-security is increasingly becoming a **priority** for all companies – in the future, this necessity may change;
- Companies would be looking for **compensation** allied to **protection and prevention services;**
- All companies use **brokers** for purchasing insurance – the most trusted source.

## B2C Segment – Key Insights (I/II)

### KEY INSIGHTS

#### Awareness

**Identity theft** and **fraud** are the most frequently mentioned incidents;

Parents' main concern is regarding **cyberbullying** - especially with their children's use of social media;

**Loss of information** and **financial losses** are the main consequences identified.

- Only 1 out of the 10 interviewees suffered a cyber attack – an online banking theft (through SMS scam);
- 6 out of the 10 recognize a **high probability of suffering a cyber incident** in the future – due to the increasing use of connected devices.

#### Level of Cybersecurity

Most interviewees only have basic **anti-virus protection** – and consider it to be enough for the level of risk they are exposed to.

- Most parents can monitor their **children's activity** online.

### Sample

**10** Individuals

**8** Women

**2** Men

**22** – **55** years

- ✓ Couples with children
- ✓ Couples with no children
- ✓ Singles with no children
- ✓ Single - parent families

# APPENDIX 12 – IN-DEPTH INTERVIEWS (KEY INSIGHTS)

Back to Presentation

## B2C Segment – Key Insights (II/II)

**KEY INSIGHTS**

**Cyber Insurance**

None of the interviewees has cyber insurance, mainly due to:

- **Lack of awareness:** 8 out of 10 had never thought about this option or did not even know this type of insurance.
- **Lack of necessity:** 2 out of 10 consider that their current level of protection is satisfactory.

E.g.,*" I believe in my personal life an anti-virus is enough; in a professional context I think it would make sense".*

Most interviewees recognize the **increasing importance of cybersecurity** and consider it to be a "hot topic".

8 out of 10 interviewees consider that in the future, they **might be willing to purchase cyber insurance**

Most interviewees would like to have coverage allied to **prevention** and **protection** services.

**Brokers** and **physical stores** are the preferred distribution channels for acquiring insurance.

**Sample**

**10** Individuals

**8** Women

**2** Men

**22** – **55** years

- ✓ Couples with children
- ✓ Couples with no children
- ✓ Singles with no children
- ✓ Single - parent families

## Agenda

## Survey Key Insights – B2B Segment (I/IV)

### Sample Composition

47 SMEs

**Cyber insurance**

88% | 19%

4 out of 9 not willing to replace

The following insights only contemplate 43

**Industries**

| | |
|---|---|
| Most Affected Sectors | 79% |
| Least Affected Sectors | 21% |

**Most frequent:**
- Accommodation
- Wholesale Trade
- Manufacturing
- Transportation & Warehousing

**Job Roles**

**Most frequent:**
- CTO/ IT Manager
- CEO
- Financial & Commercial Directors

**Annual Turnover**

| | |
|---|---|
| 6.98% | > €50M |
| 6.98% | €18M - €50M |
| 37% | €11M - €18M |
| 20% | €3.5M - €11M |
| 26% | €2M - €3.5M |
| 19% | €1M - €2M |

**Victims**

33% 》 More than once: 57%

**Non victims**

67%

**No. Employees**

| < 10 | 10-250 |
|---|---|
| 2% | 98% |

### Awareness

**Remember a Portuguese Cyber Incident Case?**

Yes 56%

No: 44%

Most Common

**Incidents Recognized**

**Median:** 5/8

**Most frequent:**
- Virus
- Malware
- Hacking

### Exposure & Readiness

**Dependency on IT & OT**

SCALE 1 TO 10

**Median:** 8

**Average:** 7.6

**Digital Platforms**

| | |
|---|---|
| Website | 88% |
| Social Media | 67% |
| E-commerce | 35% |
| Marketplace | 9% |

**Organizational Structure**

| | |
|---|---|
| IT Department | 51% |
| IT Security Area | 14% |
| DPO | 9% |
| CISO | 7% |

***Sources**: Surveys*

## Survey Key Insights – B2B Segment (II/IV)

### Awareness & Exposure

**Victims**

**Most common incidents**
- Malware
- Virus
- Hacking
- Ransomware
- Trojan

**Motivations of the attacks**
- Cyber Extortion 64%
- Cyber Espionage 14%

**Major Consequences**

Actual
1. Business Interruption
2. Asset Losses
3. Employee Motivation
4. Compliance
5. Reputational

**Non victims**

**Perceived Level of Threat**

SCALE 1 TO 10

**Median:** 5

**Average:** 4.4

**Reasons for exposure**
- Low Security
- Company's size
- Sensitive Info
- Brand Value

**Major Consequences**

Most Feared
1. Business Interruption
2. Asset Losses
3. Compliance costs
4. Reputational damages
5. Employee Motivation

### Post-incident Response

**Victims**

**Entity to which the incident was reported**
- 79 %
- 29%

**Cyber Incident Management**

| | |
|---|---|
| Internally | 42% |
| Cybersecurity Partners | 33% |
| Contracting Suppliers | 8% |

**Impact on enterprise perspective**

SCALE 1 TO 10

**Median:** 7

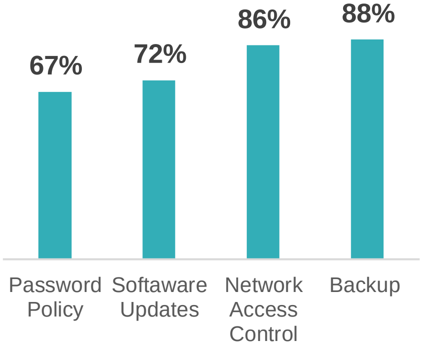
**Average:** 6.6

### Readiness

**Risk Assessment Measures**

| | |
|---|---|
| Vulnerability Diagnosis | 58% |
| Compliance Evaluation | 56% |
| Security Tests | 44% |

**Mitigation Measures**




**Contingency Norms**

| | |
|---|---|
| Incident Responses Plan | 14% |
| Monitoring Cyber Risk | 44% |
| Review and Update of Security Measures | 47% |

**Monitoring Entity**
- IT & Cybersecurity Providers
- IT Consultants

*Sources: Surveys*

## Survey Key Insights – B2B Segment (III/IV)

### W/ Cyber Insurance

**Motivations to Purchase**

| | |
|---|---|
| Company's size | 22% |
| Brand Value | 22% |
| Digital Transf. | 22% |
| Occurrence of a Cyber Attack | 22% |
| Sensitive info | 11% |

**Key Factors in Selection**

1. Coverage
2. Trust in Insurer
3. Price
4. Additional Services
5. Application Form

**Access to a Risk Assessment Tool**

Yes 1/5

No: 4/5

**Application Form**

SCALE 1 TO 5

| | | |
|---|---|---|
| Extension | 3 | 3 |
| Language | 3 | 5 |

Willingness to pay a fee for personalized assistance in filing the application form:

No 3/5

Do not Know 2/5

**Distribution Channels**

The enterprise contacted an agent

3/5

**Satisfaction Level**

0%

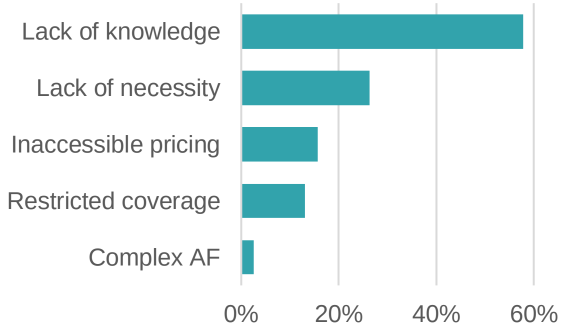
0%

100%

0%

### No Cyber Insurance

**Reasons for not having insurance**




**Most wanted cyber insurance features**

Risk Assessment
- Vulnerability Diagnoses
- Pen Tests
- Compliance Evaluation

Coverage (costs)
- Assets recovery
- Business Interruption
- Fraud/Theft

Risk Mitigation
- Employee Training
- Data Back-up
- Periodic Monitoring
- Incident Response Plan

Assistance services
- Technical Assistance
- Legal Assistance

**Distribution Channels**

| Specialized Agent | General Agent | Online |
|---|---|---|
| 66% | 11% | 5% |

**Relevance of a Risk Assessment Tool**

SCALE 1 TO 5

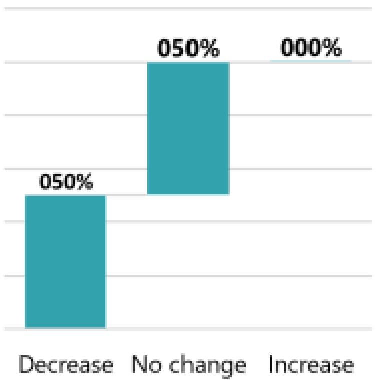
**Median: 4**

*Sources: Surveys*

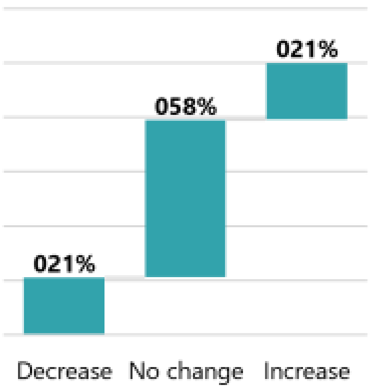
## Survey Key Insights – B2B Segment (IV/IV)

### Perceived Level of Security

**W/ Cyber Insurance**




**No Cyber Insurance**

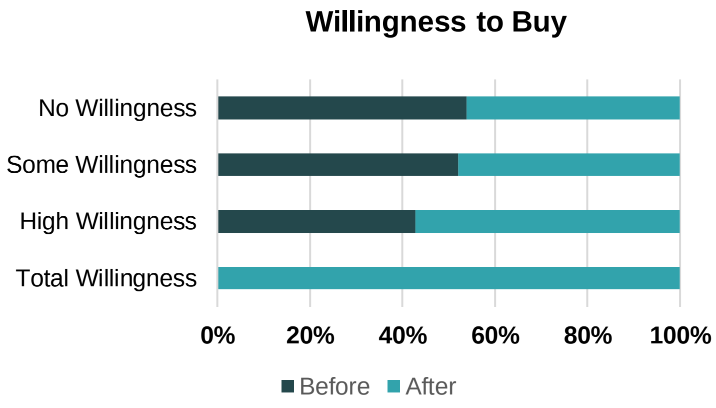



### Willingness to Buy/Replace

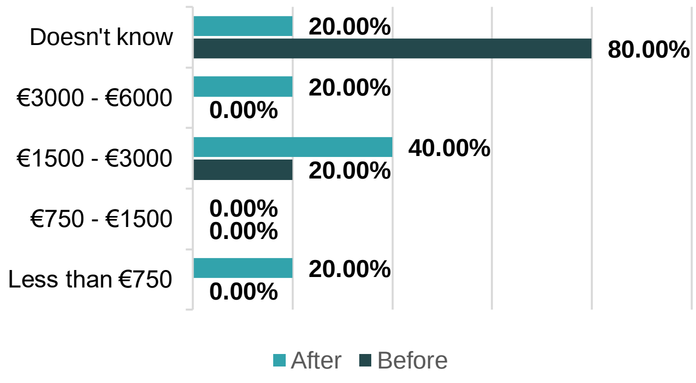
**5** Enterprises willing to replace their current cyber risk insurance

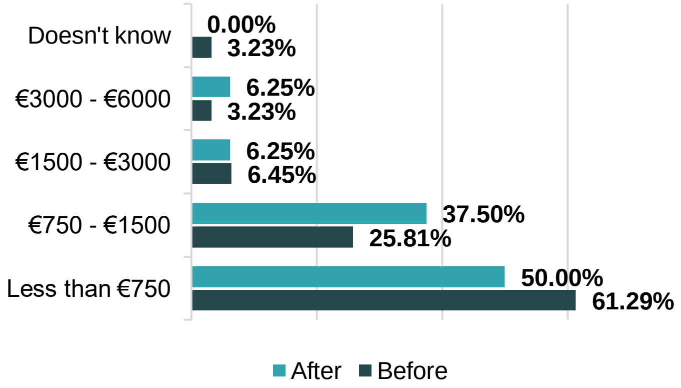
**Most wanted cyber insurance features**

| Risk Assessment | Risk Mitigation | Coverage (costs) |
|---|---|---|
| • Online risk assessment tool<br>• Vulnerability Analysis<br>• Pen Tests | • Data back-ups | • Asset loss recovery<br>• Business interruption<br>• Theft/fraud |




### Willingness to Pay



## Survey Key Insights – B2C Segment (I/V)

### Sample Composition

**525 respondents**

#### Gender Distribution

60%

40 %

#### Parent with underage children

17%

#### Household Composition

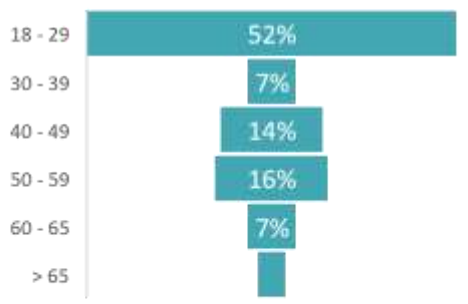
12%

24%

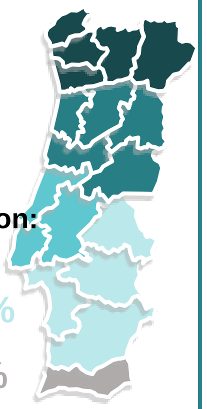
55%

9%

#### Age Distribution




#### Residence Area



North: 2%

Center: 13%

Metropolitan Area of Lisbon: 73%

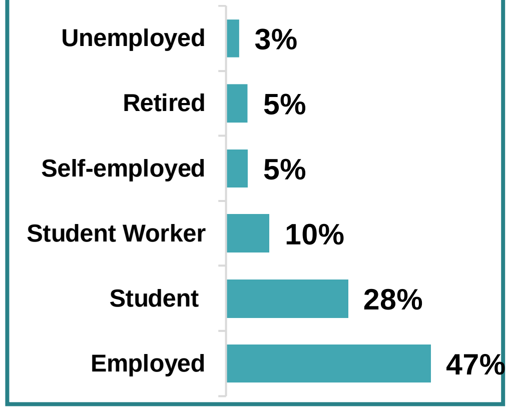
Alentejo: 4%

Algarve: 2%

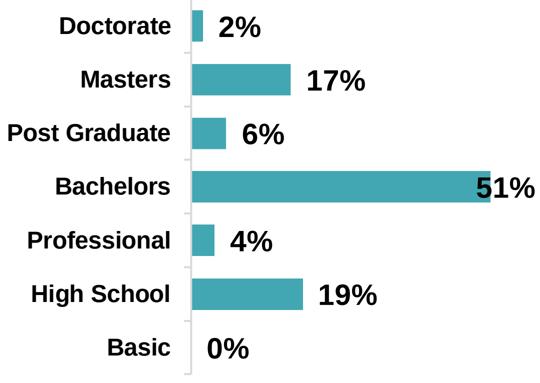
Azores: 6%

Madeira: 0%

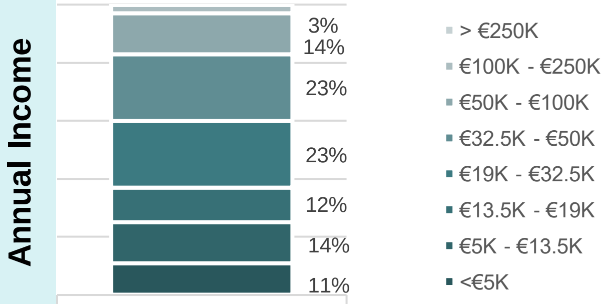
#### Occupation




#### Academic Background




#### Annual Income




#### Victims

16%

#### Non victims

84%

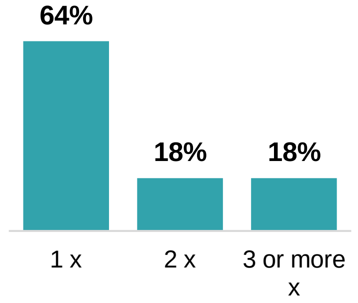
## Survey Key Insights – B2C Segment (II/V)

## Awareness

### Most common incidents

| | |
|---|---|
| 1 | Virus |
| 2 | Hacking |
| 3 | Malware |
| 4 | Ransomware |
| 5 | Phishing |

### Frequency of Incidents




### Major Consequences

**Victims**

Actual

| | |
|---|---|
| 1 | Loss of time |
| 2 | Financial |
| 3 | Psychological |
| 4 | Reputational |

**Non-Victims**

Most feared

| | |
|---|---|
| 1 | Financial |
| 2 | Psychological |
| 3 | Reputational |
| 4 | Loss of time |

### Objectives of cyber attacks

**Victims**

| | |
|---|---|
| 26% | Illegal access to bank credentials |
| 20% | Identity theft |
| 19% | Illegal access to personal data |
| 9,3% | Virtual harassment (e.g., cyberbullying) |

**Non-Victims**

| | |
|---|---|
| 61% | Illegal access to bank credentials |
| 30% | Identity theft |
| 6% | Virtual harassment (e.g., cyberbullying) |
| 4% | Illegal access to personal data |

## Tech-Savviness

### Perception Level of Threat

SCALE 1 TO 10

Average
4.7

### Cyber Bullying Concern

SCALE 1 TO 10

Average
6.9

### Victims of Cyber Bullying

**6%** Suffered or know someone who has suffered from cyberbullying

### Financial operations online

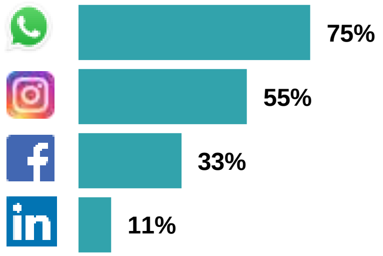
**89%** Do financial operations online

### Level of Dependency on Internet

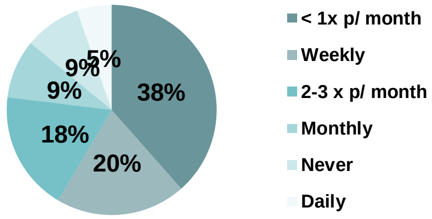
SCALE 1 TO 10

Average
7.3

### Most Daily Used Social Media



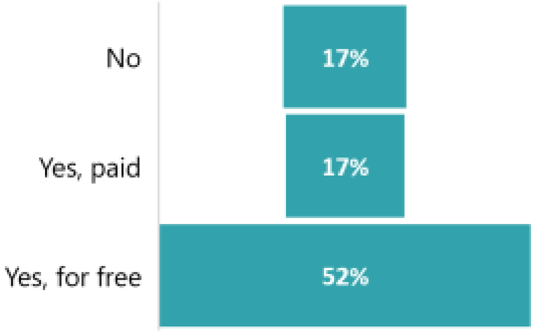

### Posting on social media



## Survey Key Insights – B2C Segment (III/V)

# Readiness

### Security in Devices



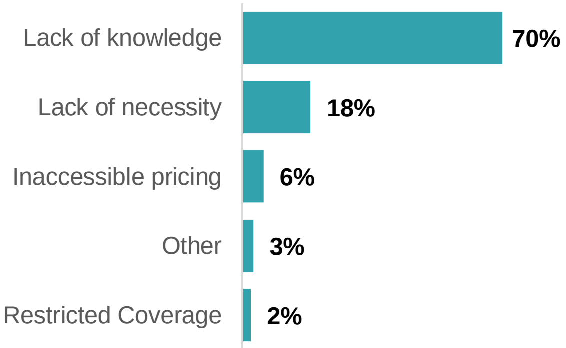

| | | |
|---|---|---|
| 1 | Anti-virus | 53% |
| 2 | Back-up on a separate place | 16% |
| 3 | VPN | 13% |
| 4 | Multifactor authentication | 12% |
| 5 | Data encryption | 5% |
| 6 | Other | 1% |

### Parents

**50%** Of parents monitor their children's online activities

| | |
|---|---|
| Monitor activities on online platforms (e.g. social media, games, etc.) | 44% |
| Time restrictions in the access to internet | 28% |
| Parental control apps/ software (e.g. Net Nanny, Kaspersky Safe Kids) | 25% |

### Reasons for not purchasing insurance




### Most wanted cyber insurance features (by order of preferences)

#### Risk Mitigation

| | |
|---|---|
| 1 | Anti-virus |
| 2 | Data back-up |
| 3 | Encryption techniques |
| 4 | Multifactor authentication |
| 5 | VPN |
| 6 | Parental control online software |

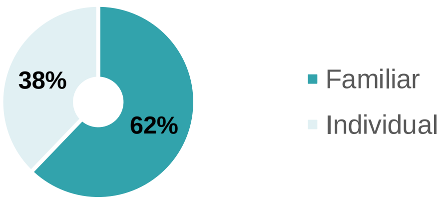
#### Coverage (costs)

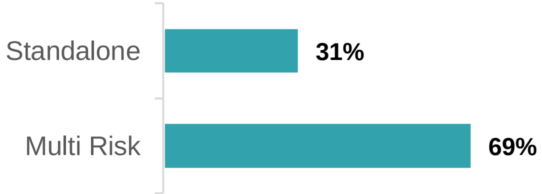
| | |
|---|---|
| 1 | Theft/Fraud Costs |
| 2 | Recovery Costs |
| 3 | Forensic Costs |

#### Assistance services

| | |
|---|---|
| 1 | Technical Assistance |
| 2 | Psychological Counseling (e.g., for cyberbullying victims) |
| 3 | Legal Assistance |

#### Structure of the Insurance



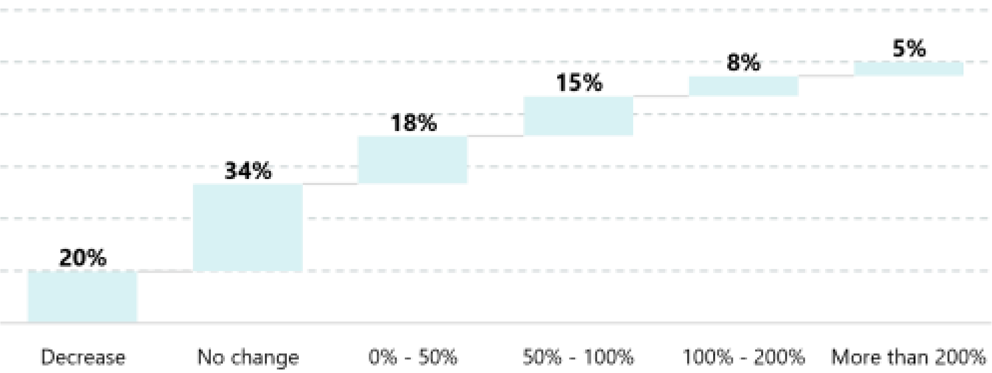

#### Distribution Channels

| | |
|---|---|
| Online | 36% |
| Physical store | 33% |
| Mobile | 14% |
| Agent | 17% |

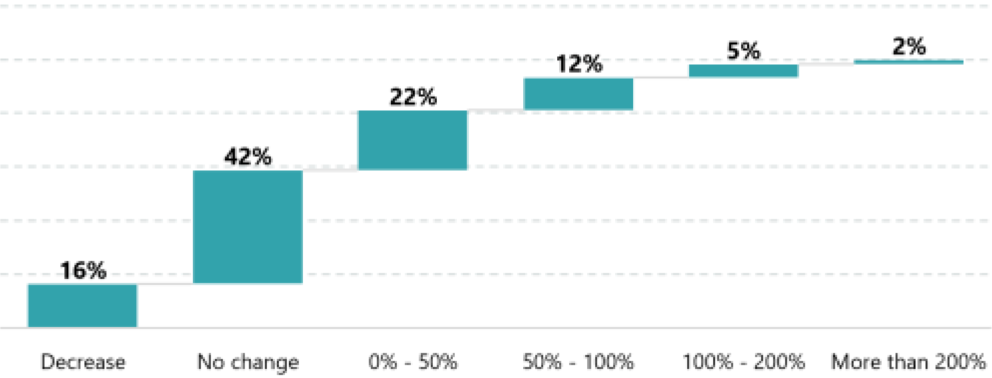
## Survey Key Insights – B2C Segment (IV/V)

### Perceived Level of Threat

**With Children**




**No Children**




### Willingness to Buy & Willingness to Pay

**Concern regarding cyberbullying**

**SCALE 1 TO 10**

| Pre-awareness | Post-awareness |
|---|---|
| Average 6.93 | Average 6.05 |

When comparing the individuals' perception regarding their level of threat before and after watching the awareness video, we can conclude the following:

- Regarding individuals with children, around 47% increased their allocated points;
- However, when asked about their level of concern with cyberbullying, the average points attributed decreased after the video;
- Concerning individuals without children, although around 42% did not change their opinions after the video, the same amount increased their allocated points.

Therefore, we can conclude that although it is fundamental to raise awareness to cyber risk, we cannot do it by explicitly instilling fear otherwise people may feel they are being manipulated.

**Sources**: *Surveys*

grupo ageas portugal

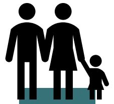
## Survey Key Insights – B2C Segment (V/V)

Back to Survey Insights

Back to “Go-To-Market” B2C

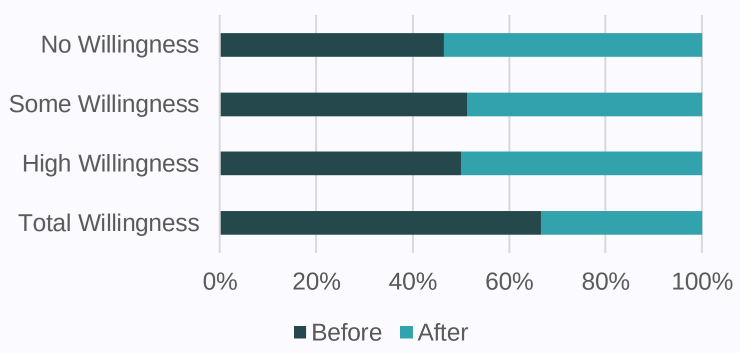
**Perceived Level of Threat**

**Willingness to Buy & Willingness to Pay**



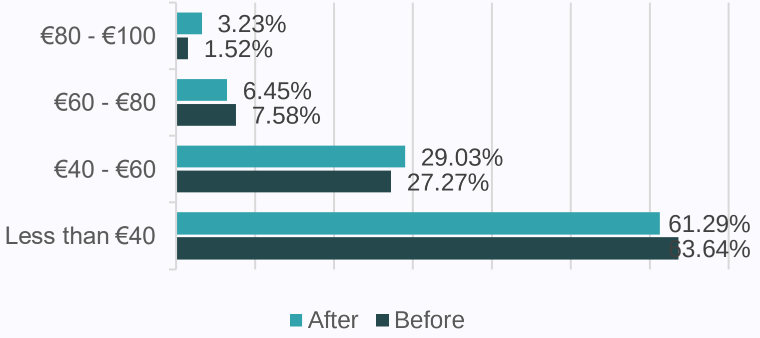
**With Children**

### Willingness to Buy

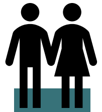



Individuals with children decreased their willingness to buy cyber insurance after watching the awareness video.

### Willingness to Pay

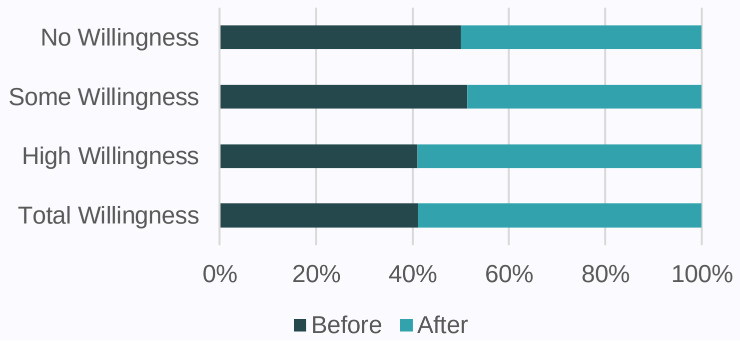



In contrast with their previous pattern, individuals with children increased their willingness to pay after the awareness video.



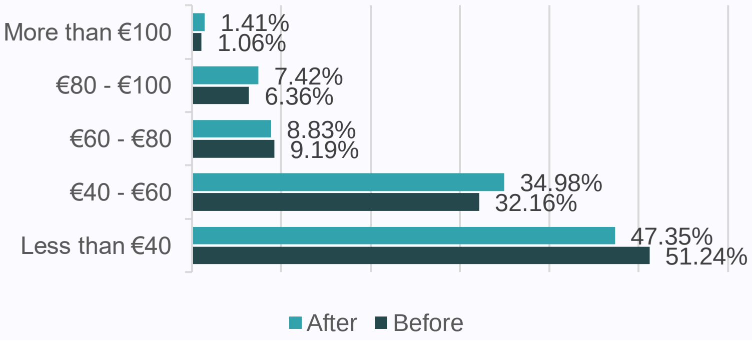
**No Children**

### Willingness to Buy




Individuals without children, on the other hand, increased their willingness to acquire this type of insurance.

### Willingness to Pay




Individuals without children slightly increased their willingness to pay, shifting the majority from “less” to ”more than €40”.

## Agenda

1 **Attribute exposure, awareness, readiness and monetary value points to create customer segments**

Variables with a negative impact

| Exposure | Weights |
|---|---|
| Cyber Victim | 20% |
| Dependency on IT/OT | 20% |
| Use of Digital Platforms | 20% |
| Number of attacks suffered | 15% |
| Industries | 15% |
| No. of collaborators | 5% |
| Perception of cyber risk | 5% |

**Standardized and Inverted Values**

Variables with a positive impact

| Awareness & Readiness | Weights |
|---|---|
| Risk Assessment Measures | 20% |
| Contingency Norms | 20% |
| Organizational structure | 15% |
| Risk Mitigation | 15% |
| Regulations and Norms | 10% |
| Remembering a Portuguese cyber incident case and specify | 10% |
| Cyber Incidents Recognized | 5% |
| Future relevance of cybersecurity | 5% |

**Standardized Values**

| Monetary Value | Weights |
|---|---|
| Willingness to Pay | 40% |
| Willingness to Buy | 40% |
| Willingness to replace (if the company has cyber insurance) | 20% |

**Standardized Values**

**Sources**: *Surveys*

# APPENDIX 14 – EAR MODEL (CLUSTERING B2B)

Back to Presentation

2 **Create customer segments (clusters) according to the calculated variables**

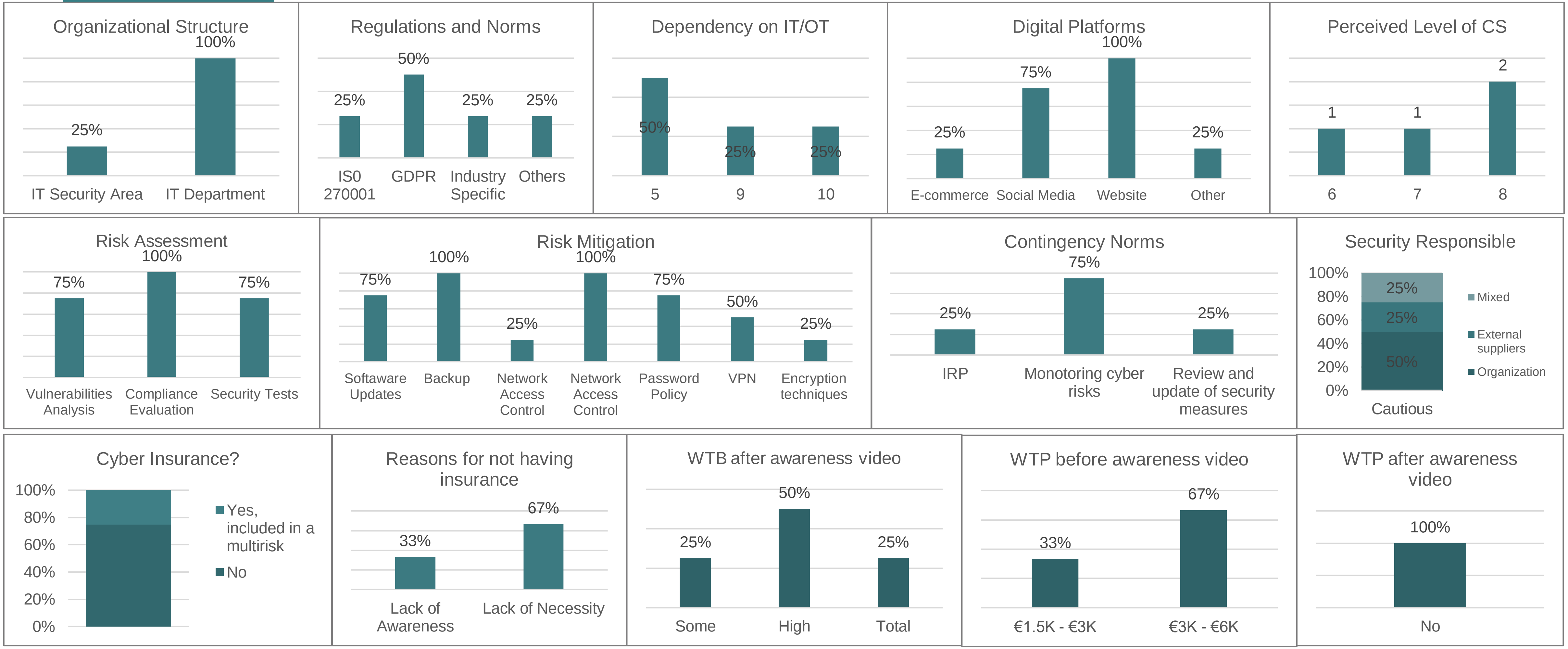
| B2B Segment | Exposure (E) | Awareness & Readiness (A) | Monetary Value (M) | Segment Name | % of Total |
|---|---|---|---|---|---|
| | Low Exposure | Low Exposure High Awareness and Readiness | Low E, High AR, High Monetary | **Cautious** | **9.3%** |
| | | | Low E, High AR, Low Monetary | **Mindful** | **11.6%** |
| | | Low Exposure Low Awareness and Readiness | Low E, Low AR, High Monetary | **High Roller** | **4.7%** |
| | | | Low E, Low AR, Low Monetary | **Unplugged** | **23.3%** |
| | High Exposure | High Exposure High Awareness and Readiness | High E, High AR, High Monetary | **Prepared** | **20.9%** |
| | | | High E, High AR, Low Monetary | **Self-sufficient** | **7%** |
| | | High Exposure Low Awareness and Readiness | High E, Low AR, High Monetary | **Reliant** | **2.3%** |
| | | | High E, Low AR, Low Monetary | **Reckless** | **20.9%** |

***Sources**: Surveys*

## Agenda

# APPENDIX 15 – PROFILING CLUSTERS (B2B)

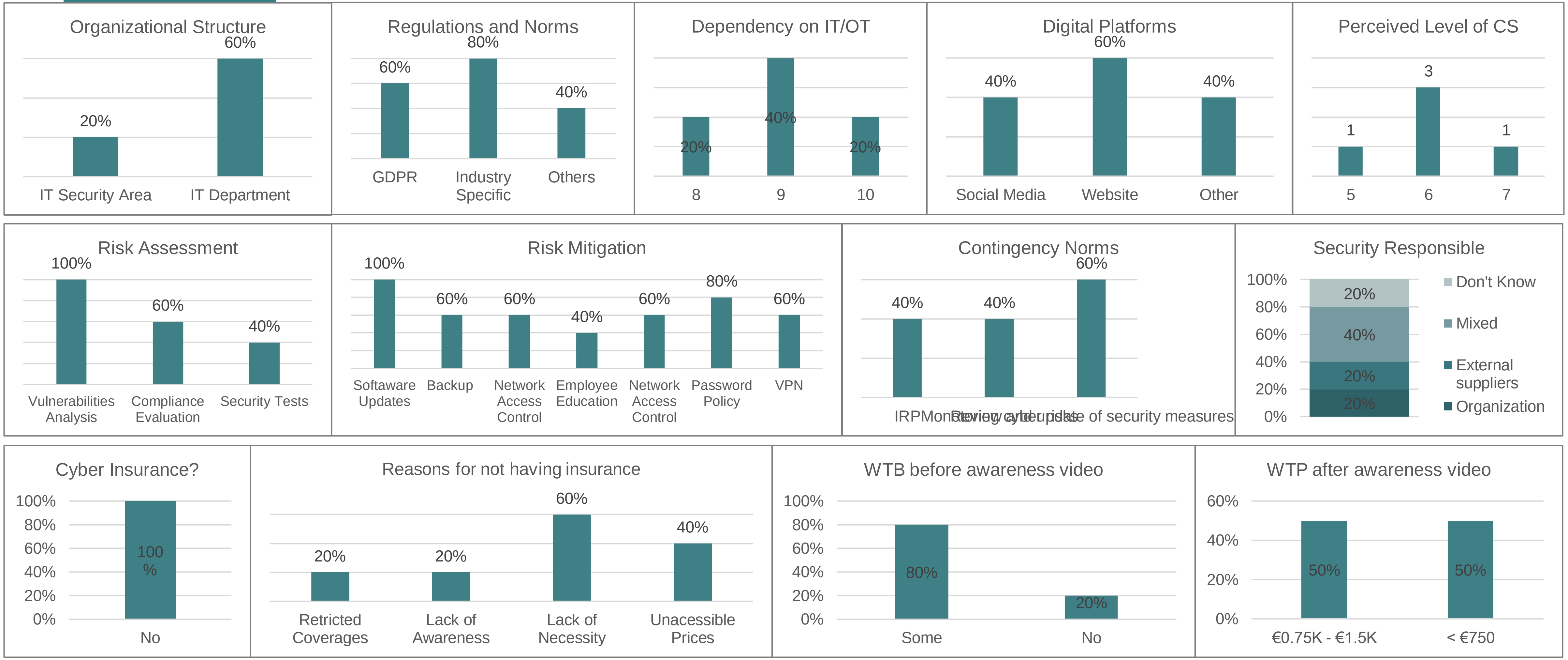
## CAUTIOUS




***Sources**: Surveys*

# APPENDIX 15 – PROFILING CLUSTERS (B2B)

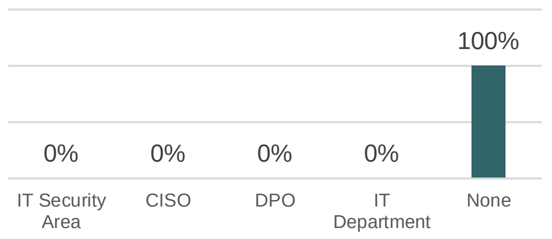
**MINDFUL**

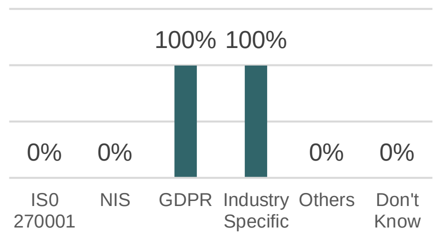


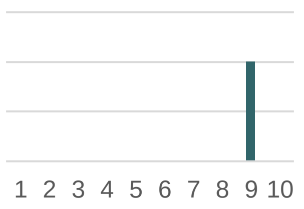

***Sources**: Surveys*

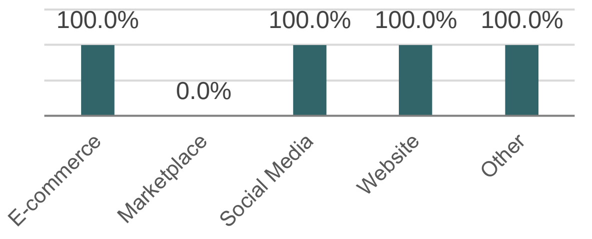
# APPENDIX 15 – PROFILING CLUSTERS (B2B)

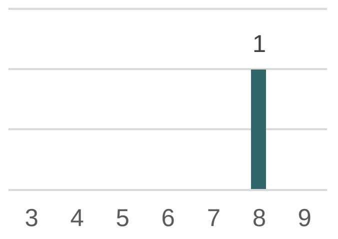
## RELIANT

### Organizational Structure



### Regulations and Norms


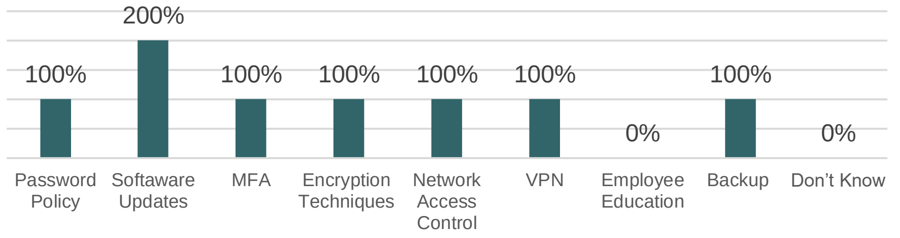

### Dependency on IT/OT


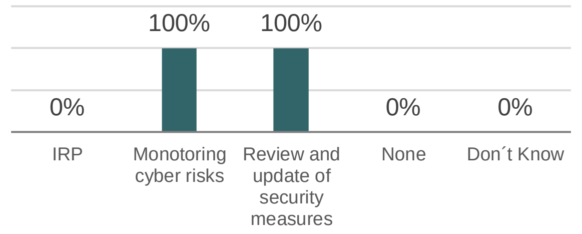

### Digital Platforms


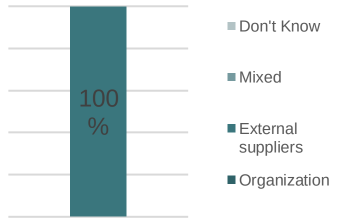

### Perceived Level of CS


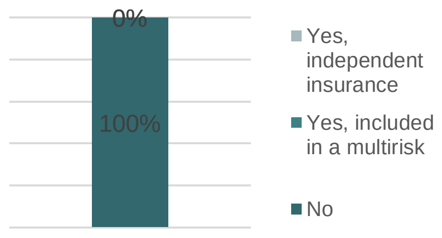

### Risk Assessment

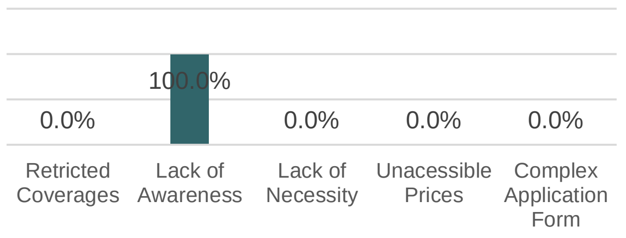


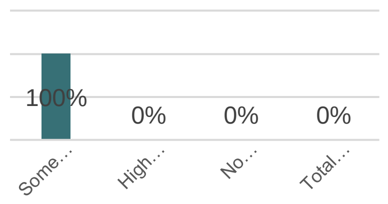
### Risk Mitigation


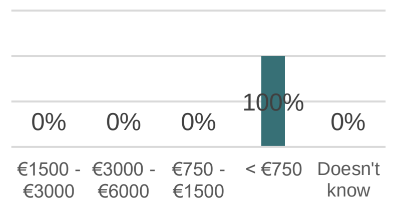

### Contingency Norms


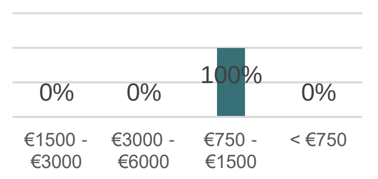

### Security Responsible



### Cyber Insurance?



### Reasons for not having insurance



### WTB before awareness video


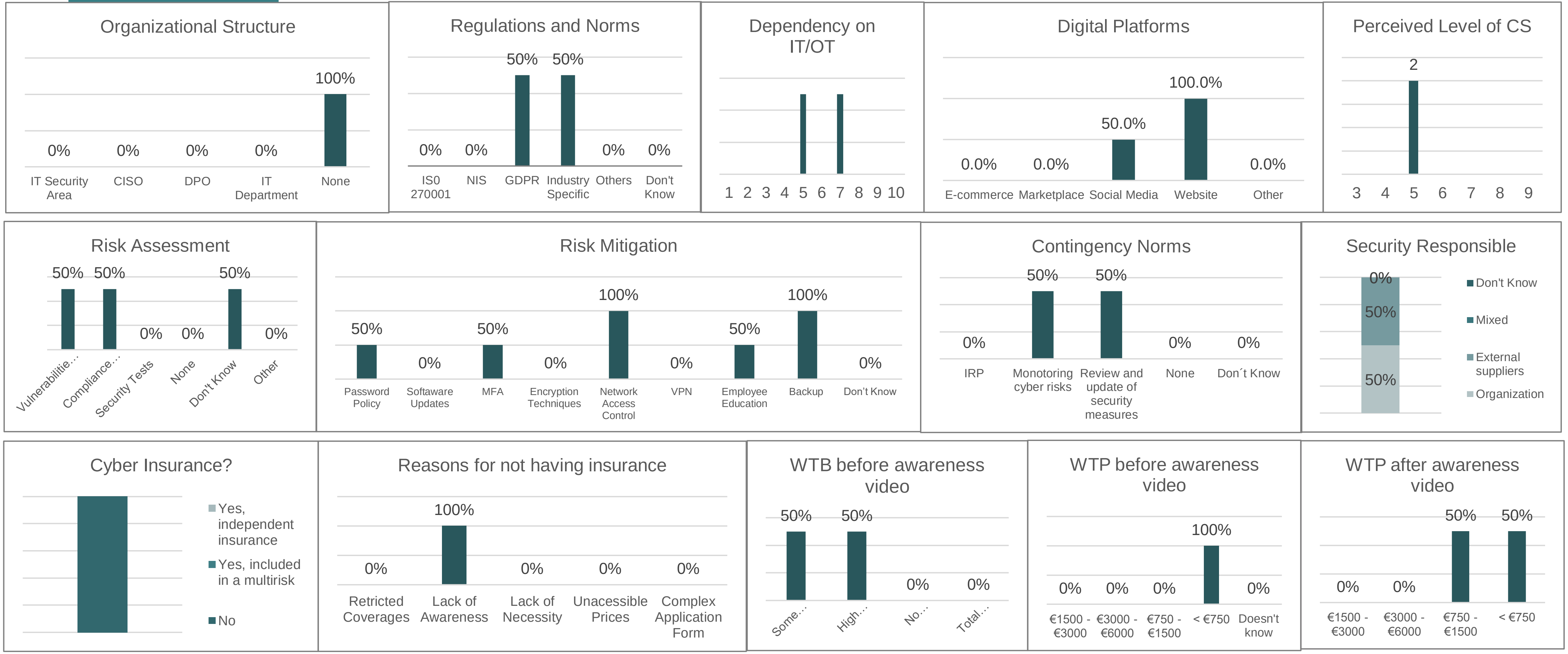

### WTP before awareness video



### WTP before awareness video



**Sources**: *Surveys*

# APPENDIX 15 – PROFILING CLUSTERS (B2B)

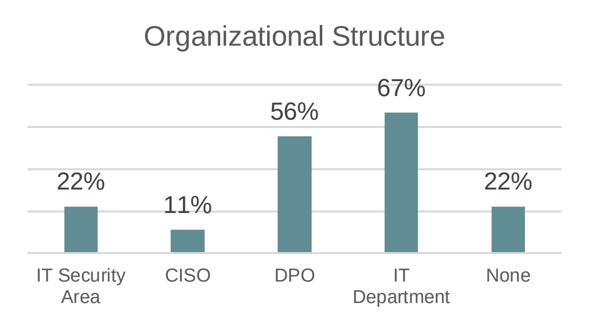
## HIGH ROLLER

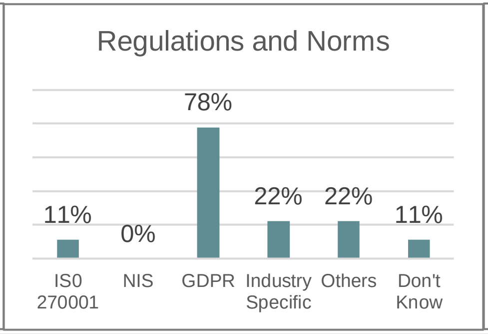


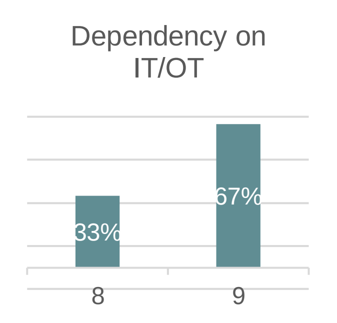

***Sources**: Surveys*

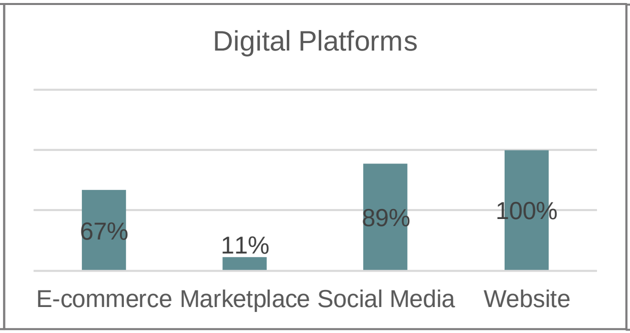
# APPENDIX 15 – PROFILING CLUSTERS (B2B)

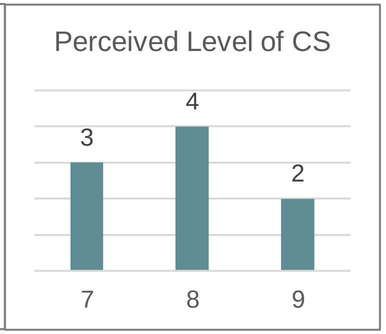
## PREPARED



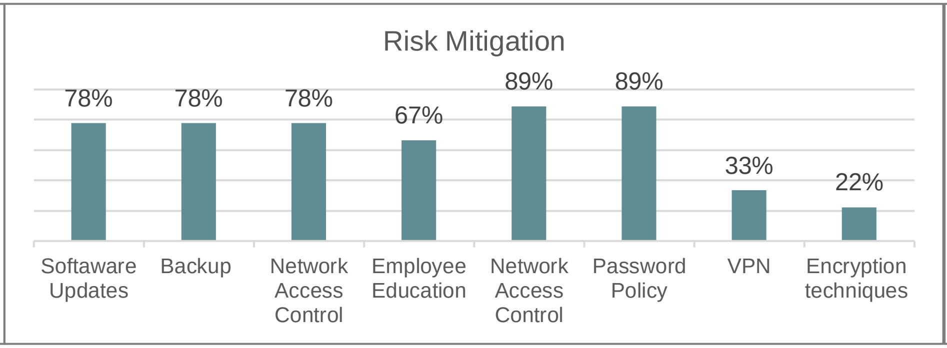



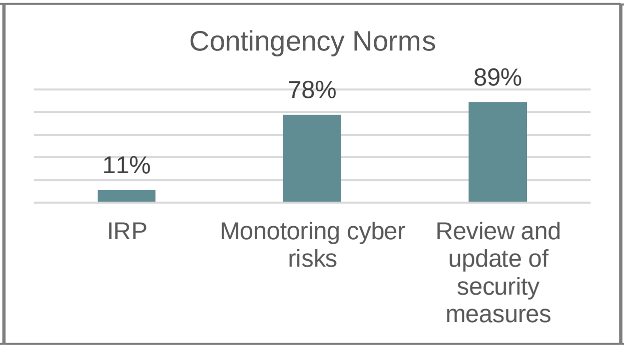



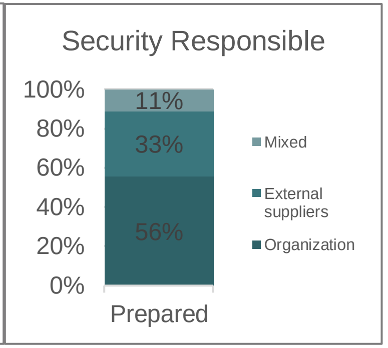



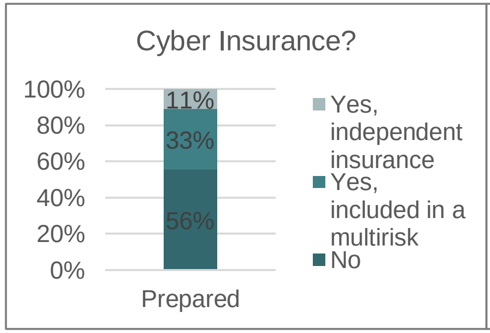



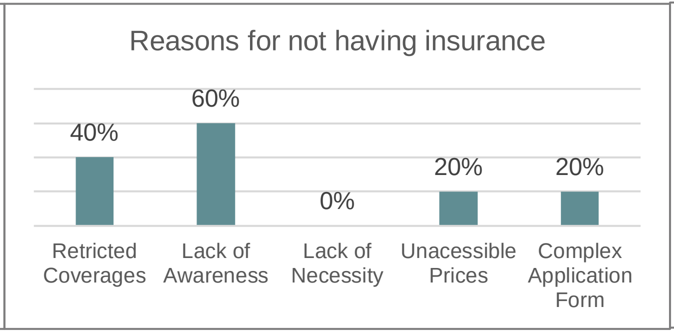


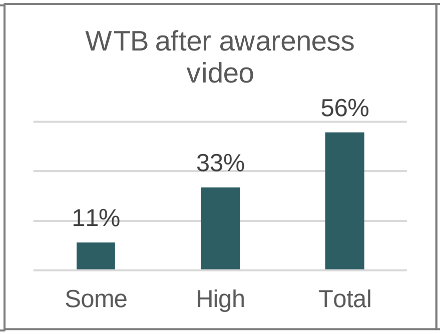


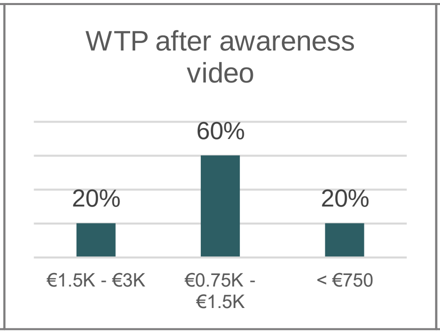



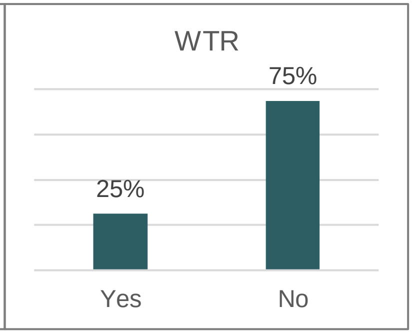



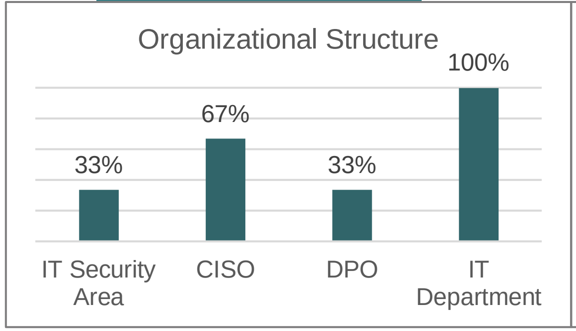



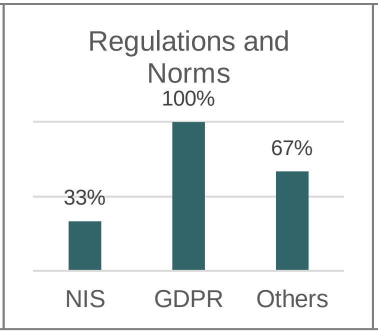



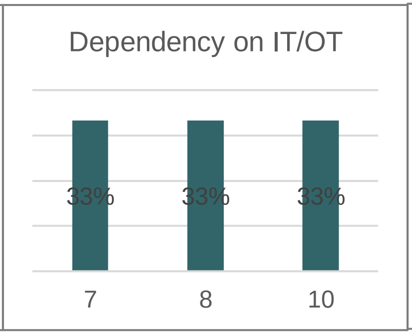

***Sources**: Surveys*

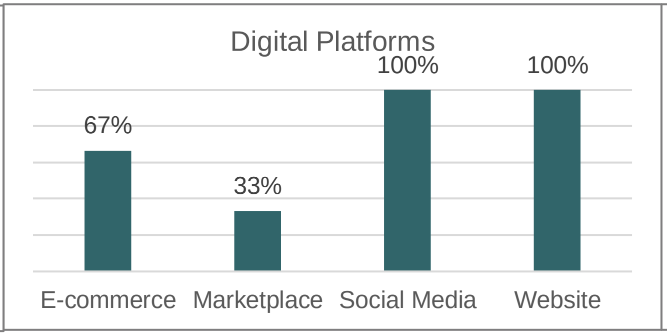
# APPENDIX 15 – PROFILING CLUSTERS (B2B)

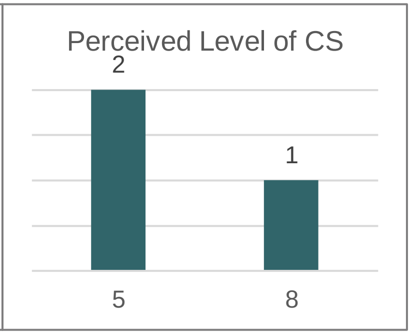
## SEL-SUFFICIENT

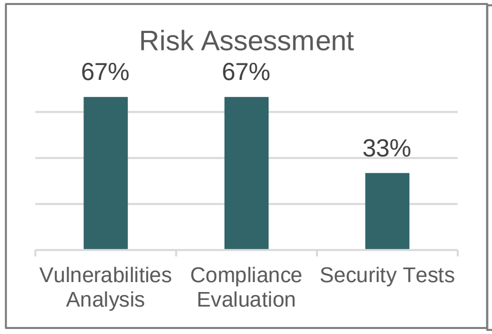


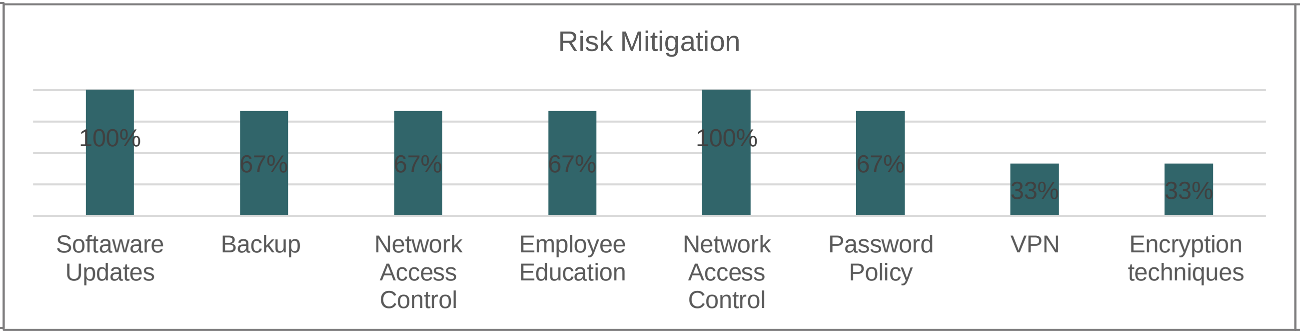



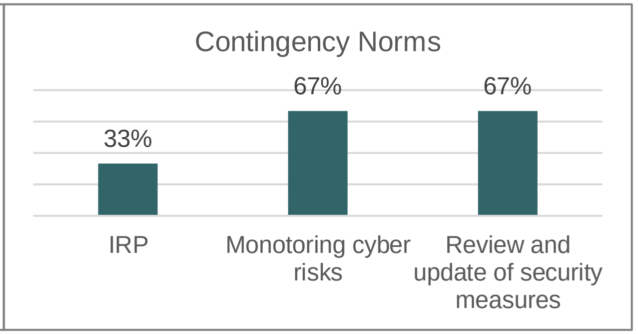



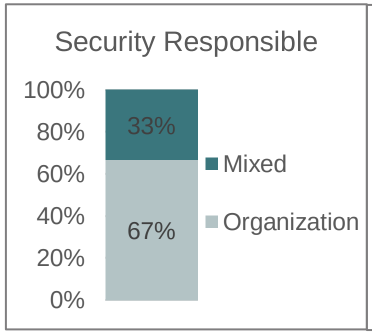



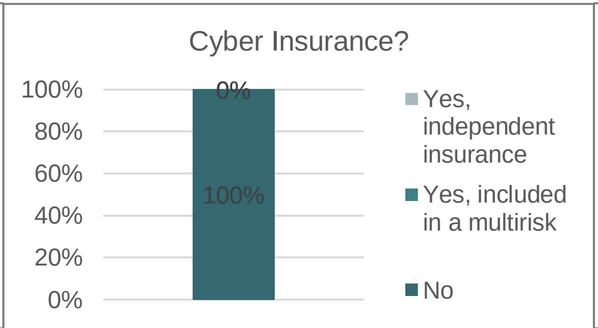



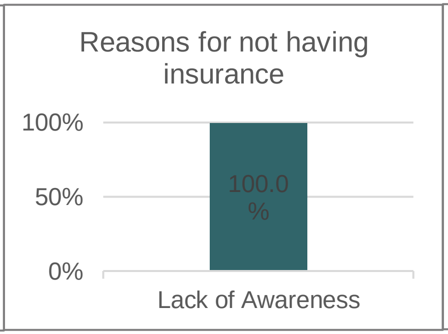



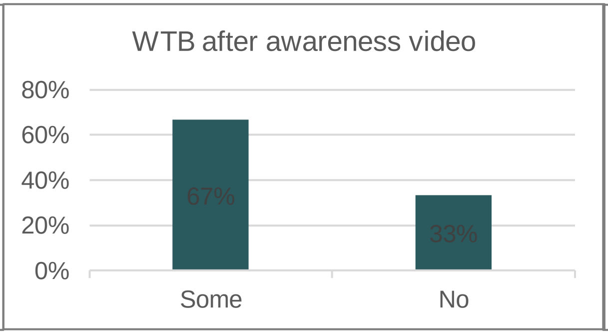



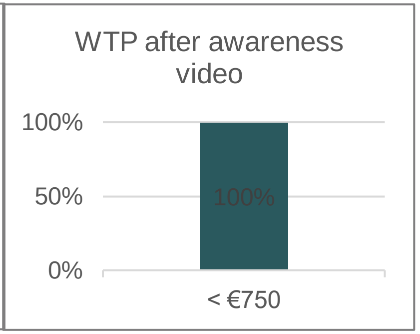



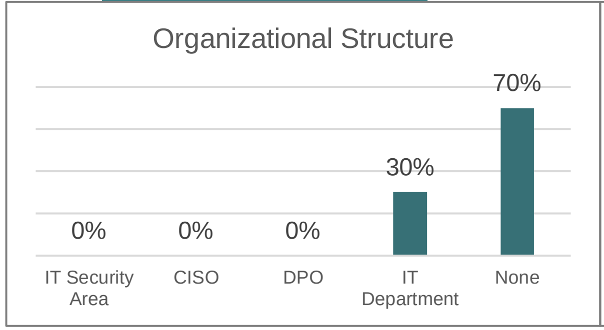



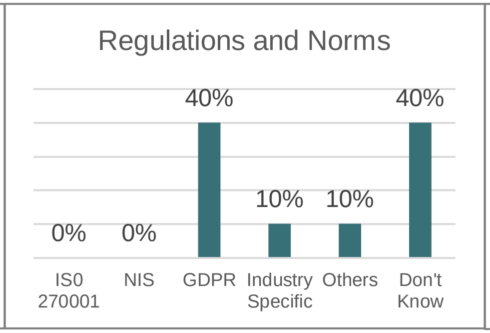

***Sources**: Surveys*

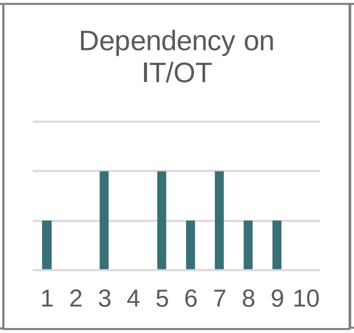
# APPENDIX 15 – PROFILING CLUSTERS (B2B)

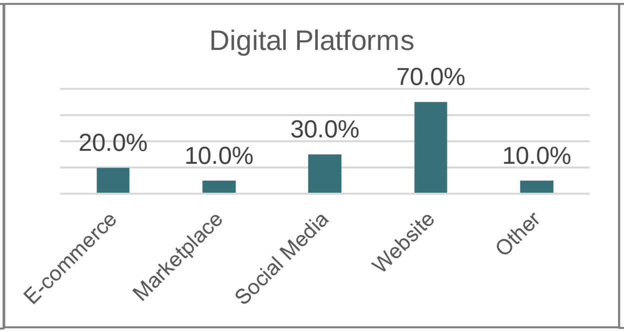
Back to Presentation

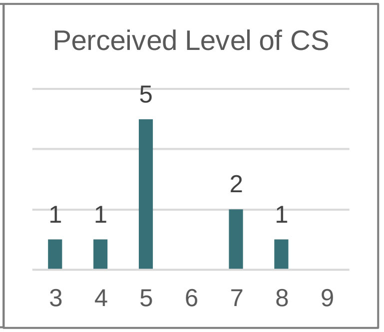
## UNPLUGGED

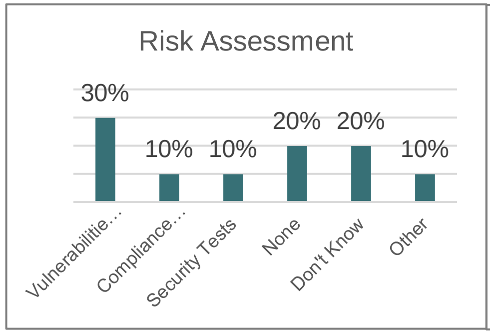


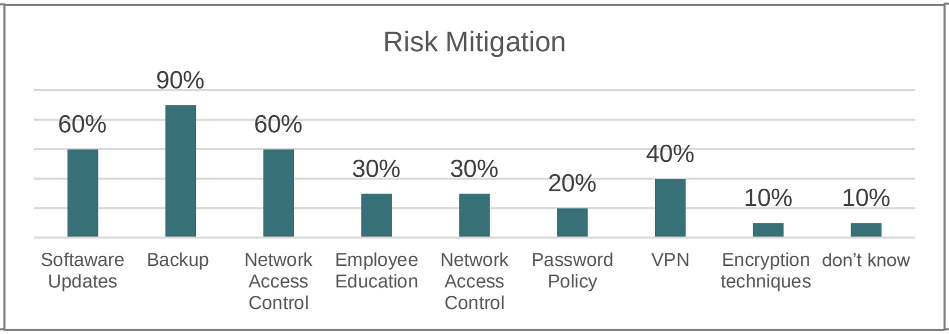



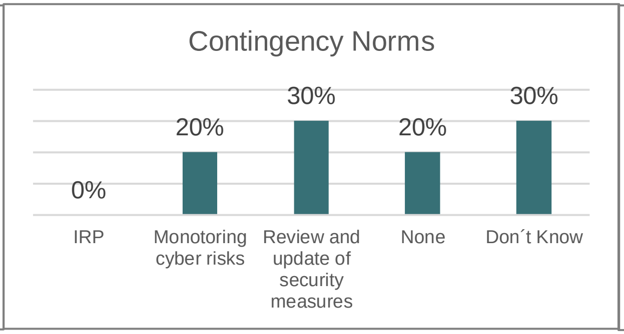



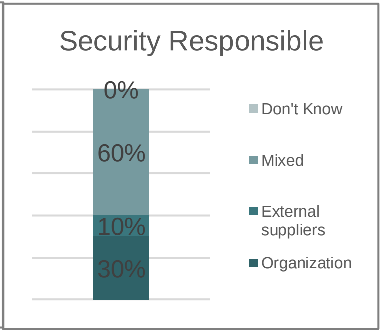



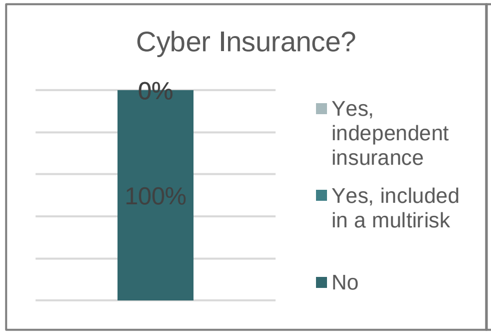



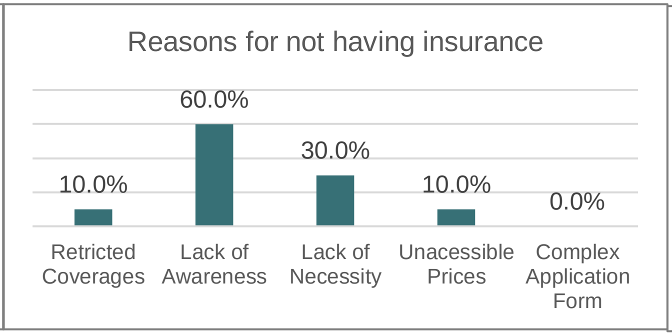



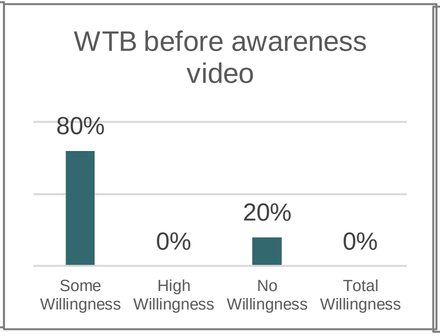



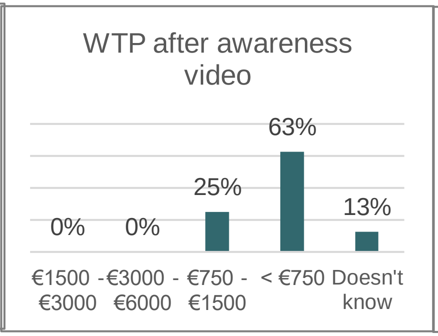



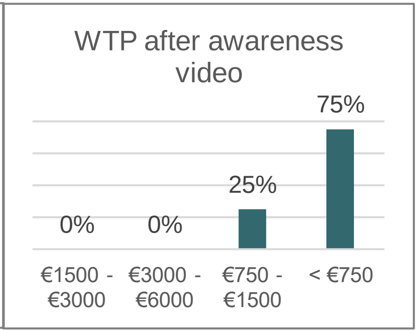



## Agenda

# APPENDIX 16 – CLUSTER SELECTION REASONING (B2B)

Back to Presentation

2 **Create customer segments (clusters) according to the calculated variables**

B2B Segment

| Segment Name | EAR |
|---|---|
| Cautious | + + + |
| Mindful | + + - |
| High Roller | + - + |
| Unplugged | + - - |
| Prepared | - + + |
| Self-sufficient | - + - |
| Reliant | - - + |
| Reckless | - - - |

**Selection Reasoning**

The "Reliant" segment only accounted for one company. Its similarity with the "High Roller" segment allowed for an association of these two segments.

The low exposure of the "Unplugged" segment together with low awareness and monetary value makes this the segment with the lowest potential for cyber insurance.

The high level of exposure together with the low level of awareness and low willingness to buy of the "Reckless" segment originates a *recipe for disaster*

**Sources**: *Surveys*

## Agenda

# APPENDIX 17 – CUSTOMER PERSONAS(B2B)

## CAUTIOUS

**Low Exposure**
**High Awareness**
**High Monetary Value**

| IT Departments/Roles | Regulations & Norms |
|---|---|
| • IT Department<br>• IT Security Area | Follows ISO 27001<br>• Industry specific regulations |

**Main Characteristics**

- Medium level of dependency on IT/OT;
- None of the surveyed companies have been attacked;
- High perceived level of cybersecurity;
- #2 in risk assessment measures;
- 1/4 have cyber risk insurance.

| WTB | WTP |
|---|---|
| High | High |

## MINDFUL

**Low Exposure**
**High Awareness**
**Low Monetary Value**

| IT Departments/Roles | Regulations & Norms |
|---|---|
| • IT Department<br>• IT Security Area | • Industry specific regulations |

**Main Characteristics**

- High level of dependency on IT/OT;
- None of the surveyed companies have been attacked;
- Main reason behind the high level of threat: sensitive and high-value information;
- Medium perceived level of cybersecurity;
- #3 in risk assessment measures;

| WTB | WTP |
|---|---|
| High | High |

**Sources**: *Surveys*

# APPENDIX 17 – CUSTOMER PERSONAS(B2B)

## RELIANT

**Medium Exposure**
**Low Awareness**
**High Monetary**

| IT Departments/Roles | Regulations & Norms |
|---|---|
| • None | • Industry specific regulations |

**Main Characteristics**

- Medium level of dependency on IT/OT;
- Medium level of perceived cybersecurity;
- Most security measures are outsourced;

| WTB | WTP |
|---|---|
| High | Medium |

## PREPARED

**High Exposure**
**High Awareness**
**High Monetary Value**

| IT Departments/Roles | Regulations & Norms |
|---|---|
| • IT Department<br>• IT Security Area<br>• CISO<br>• DPO | Follows ISO 27001<br>• Industry specific regulations |

**Main Characteristics**

- High level of dependency on IT/OT;
- #1 in number of cyber-attacks;
- High perceived level of cybersecurity;
- #1 in risk assessment measures;
- #2 in contingency norms;
- 4/9 have cyber risk insurance.

| WTB | WTP |
|---|---|
| High | High |

**Sources**: *Surveys*

# APPENDIX 17 – Customer Personas (B2B)

Back to Presentation

## SELF SUFFICIENT

**High Exposure**
**High Awareness**
**Low Monetary Value**

**IT Departments/Roles**

- IT Department
- IT Security Area
- CISO
- DPO

**Regulations & Norms**

- Other regulations

**Main Characteristics**

- High level of dependency on IT/OT;
- #2 in number of cyber-attacks;
- #1 in incidents recognized;
- Main reason behind the high level of threat: brand image and sensitive and high-value information;
- Medium level of perceived cybersecurity;
- Internalized cybersecurity services.

| WTB | WTP |
|---|---|
| Medium | Low |

## UNPLUGGED

**High Exposure**
**Low Awareness**
**Low Monetary**

**IT Departments/Roles**

- IT Department

**Regulations & Norms**

- Companies do not know the regulations

**Main Characteristics**

- Low level of dependency on IT/OT;
- Low number of cyber-attacks;
- Low perceived level of cybersecurity;
- Main reason behind the high level of threat: low cybersecurity
- Last in risk assessment measures.

| WTB | WTP |
|---|---|
| Low | Low |

***Sources**: Surveys*

## Agenda

1 **Attribute tech-savviness, awareness, readiness and monetary value points to create customer segments**

Variables with a positive impact

| Tech-Savviness | Weights |
|---|---|
| Dependency on the internet | 25% |
| Usage of financial operations | 20% |
| Usage of social media | 20% |
| Frequency of personal content | 10% |
| Degree of social media privacy | 15% |
| Sharing/storing files | 10% |

| Awareness & Readiness | Weights |
|---|---|
| Cyber attack/cyberbullying victim | 25% |
| Refrainment from Risky behaviours | 15% |
| Knows a cyber attack/cyberbullying victim | 15% |
| Security measures online | 15% |
| Security Services on Devices | 10% |
| Protection Measures | 15% |
| Perception of cyber risk | 5% |

| Monetary Value | Weights |
|---|---|
| Willingness to Buy | 50% |
| Willingness to Pay | 50% |

**Standardized Values**

**Standardized Values**

**Standardized Values**

**Sources**: *Surveys*

# APPENDIX 18 – TAR MODEL (CLUSTERING B2C)

Back to Presentation

2 **Create customer segments (clusters) according to the calculated variables**

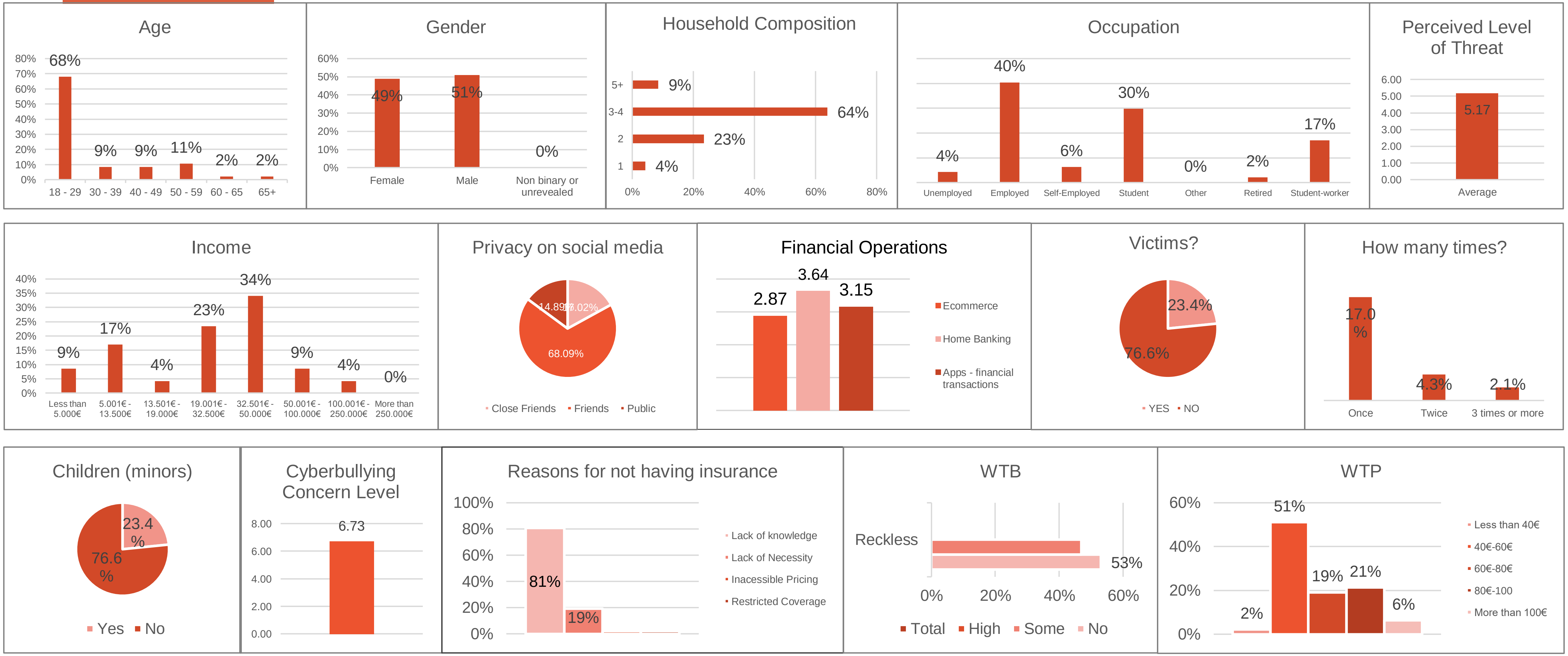
| B2C Segment | Tech- Savviness (T) | Awareness & Readiness (A) | Monetary Value (M) | Segment Name | % of Total |
|---|---|---|---|---|---|
| | High Tech Savviness | High Tech Savviness High Awareness and Readiness | High T, High A, High Monetary | **Ready** | **9%** |
| | | | High T, High A, Low Monetary | **Miss Independent** | **13.5%** |
| | | High Tech Savviness Low Awareness and Readiness | High T, Low A, High Monetary | **Big-spender** | **10.9%** |
| | | | High T, Low A, Low Monetary | **Chance-taker** | **15.8%** |
| | Low Tech Savviness | Low Tech Savviness High Awareness and Readiness | Low T, High A, High Monetary | **Prudent** | **9%** |
| | | | Low T, High A, Low Monetary | **Alert** | **18.5%** |
| | | Low Tech Savviness Low Awareness and Readiness | Low T, Low A, High Monetary | **Misfit** | **6.1%** |
| | | | Low T, Low A, Low Monetary | **Disconnected** | **17.3%** |

***Sources**: Surveys*

## Agenda

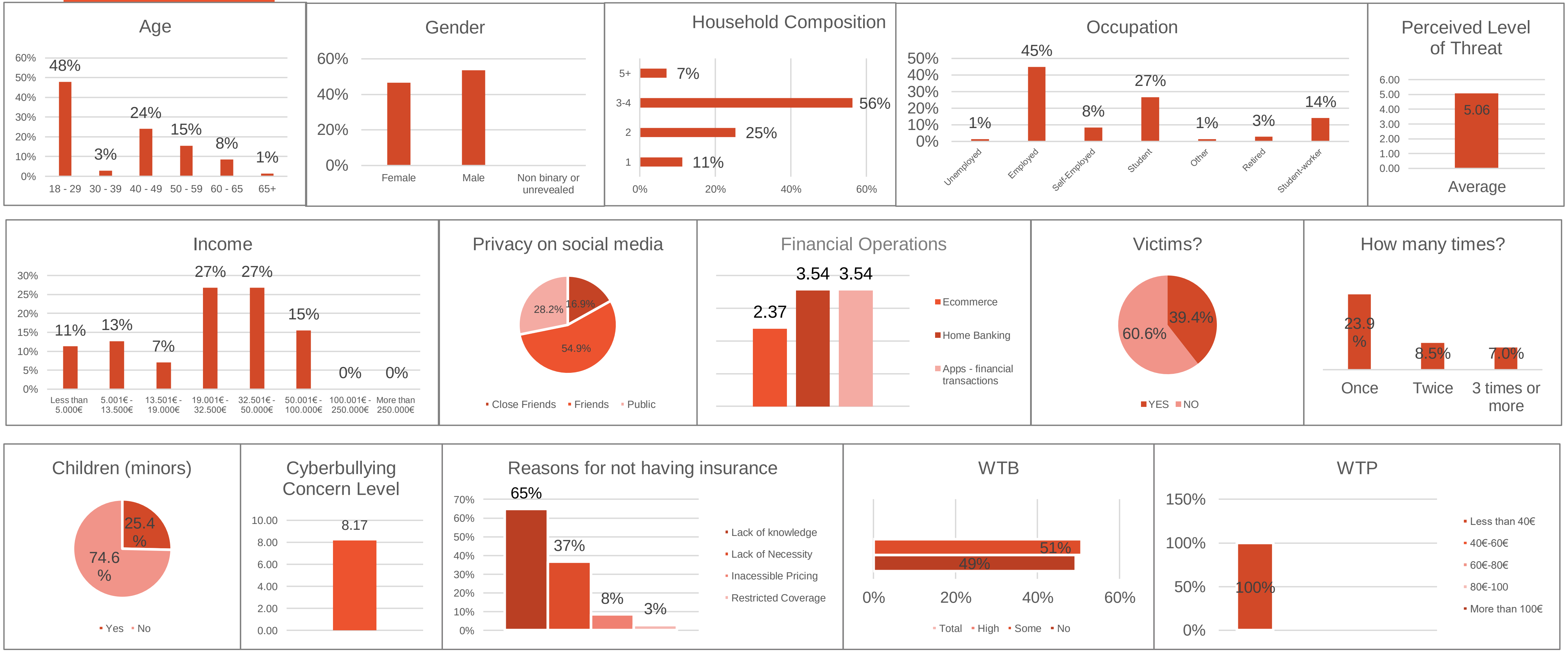
# APPENDIX 19 – PROFILING CLUSTERS (B2C)

READY



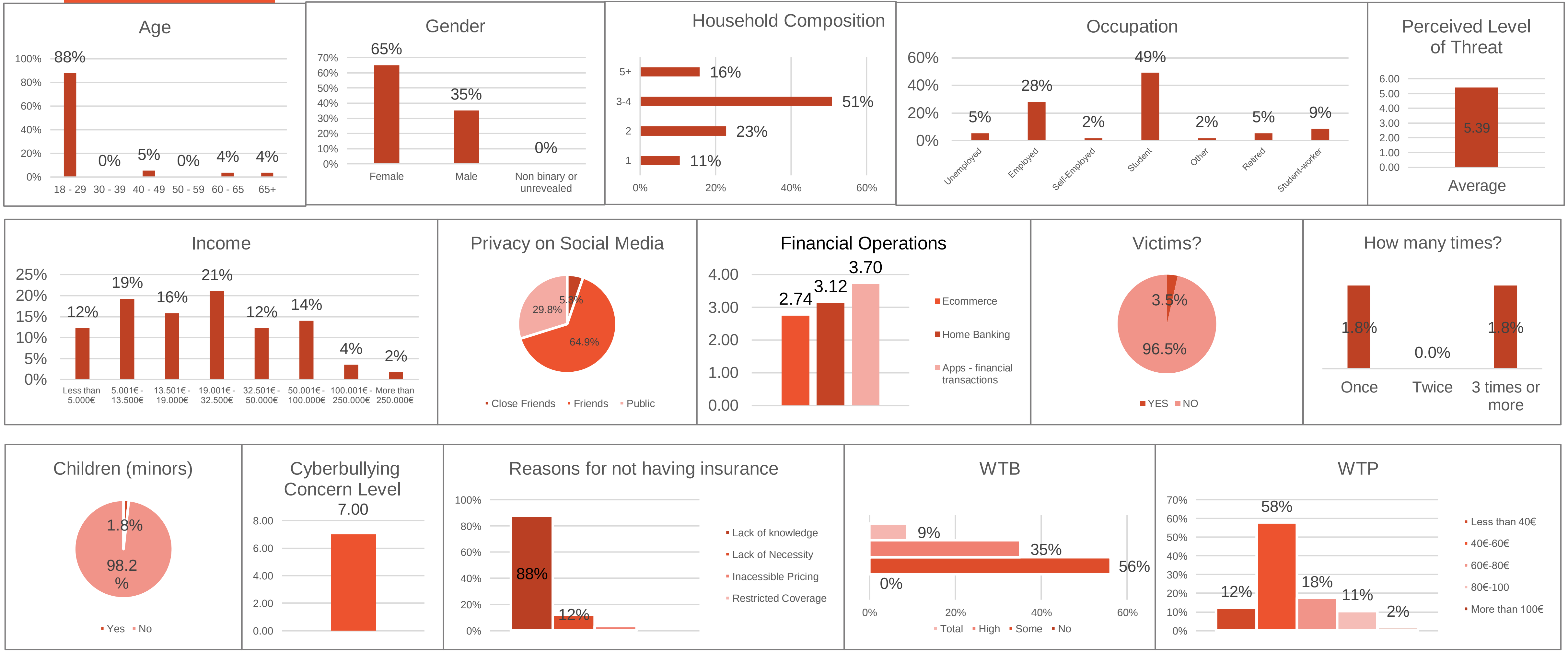
# APPENDIX 19 – PROFILING CLUSTERS (B2C)

**MISS INDEPENDENT**




**Sources**: *Surveys*

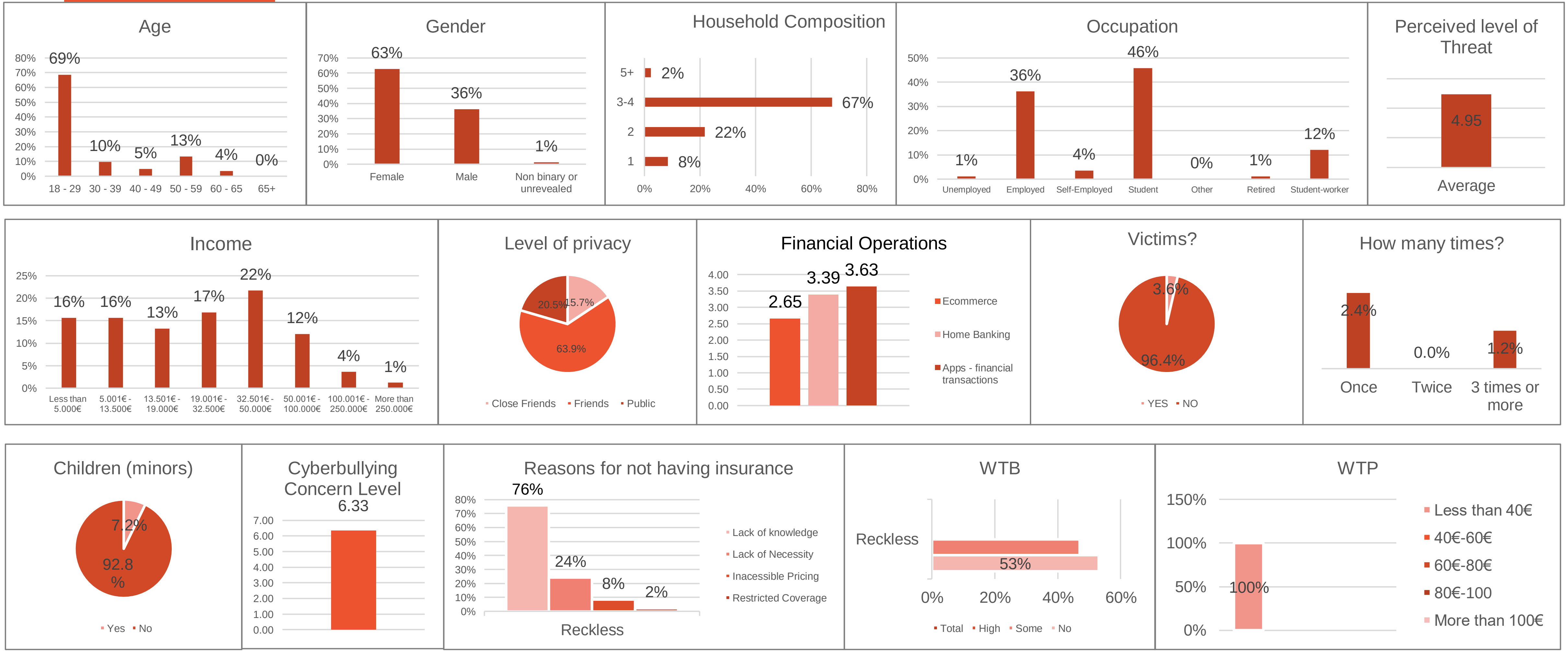
BIG SPENDER



Age
100% 80% 60% 40% 20% 0%
88% 0% 5% 0% 4% 4%
18 - 29 30 - 39 40 - 49 50 - 59 60 - 65 65+
Gender
70% 60% 50% 40% 30% 20% 10% 0%
65% 35% 0%
Female Male Non binary or unrevealed
Household Composition
5+ 16%
3-4 51%
2 23%
1 11%
0% 20% 40% 60%
Occupation
60% 40% 20% 0%
5% 28% 2% 49% 2% 5% 9%
Unemployed Employed Self-Employed Student Other Retired Student-worker
Perceived Level of Threat
6.00 5.00 4.00 3.00 2.00 1.00 0.00
5.39
Average
Income
25% 20% 15% 10% 5% 0%
12% 19% 16% 21% 12% 14% 4% 2%
Less than 5.000€ 5.001€ - 13.500€ 13.501€ - 19.000€ 19.001€ - 32.500€ 32.501€ - 50.000€ 50.001€ - 100.000€ 100.001€ - 250.000€ More than 250.000€
Privacy on Social Media
5.3% 29.8% 64.9%
Close Friends Friends Public
Financial Operations
4.00 3.00 2.00 1.00 0.00
2.74 3.12 3.70
Ecommerce
Home Banking
Apps - financial transactions
Victims?
3.5% 96.5%
YES NO
How many times?
1.8% 0.0% 1.8%
Once Twice 3 times or more
Children (minors)
1.8% 98.2 %
Yes No
Cyberbullying Concern Level
8.00 6.00 4.00 2.00 0.00
7.00
Reasons for not having insurance
100% 80% 60% 40% 20% 0%
88% 12%
Lack of knowledge
Lack of Necessity
Inacessible Pricing
Restricted Coverage
WTB
9% 35% 56% 0%
0% 20% 40% 60%
Total High Some No
WTP
70% 60% 50% 40% 30% 20% 10% 0%
12% 58% 18% 11% 2%
Less than 40€
40€-60€
60€-80€
80€-100
More than 100€

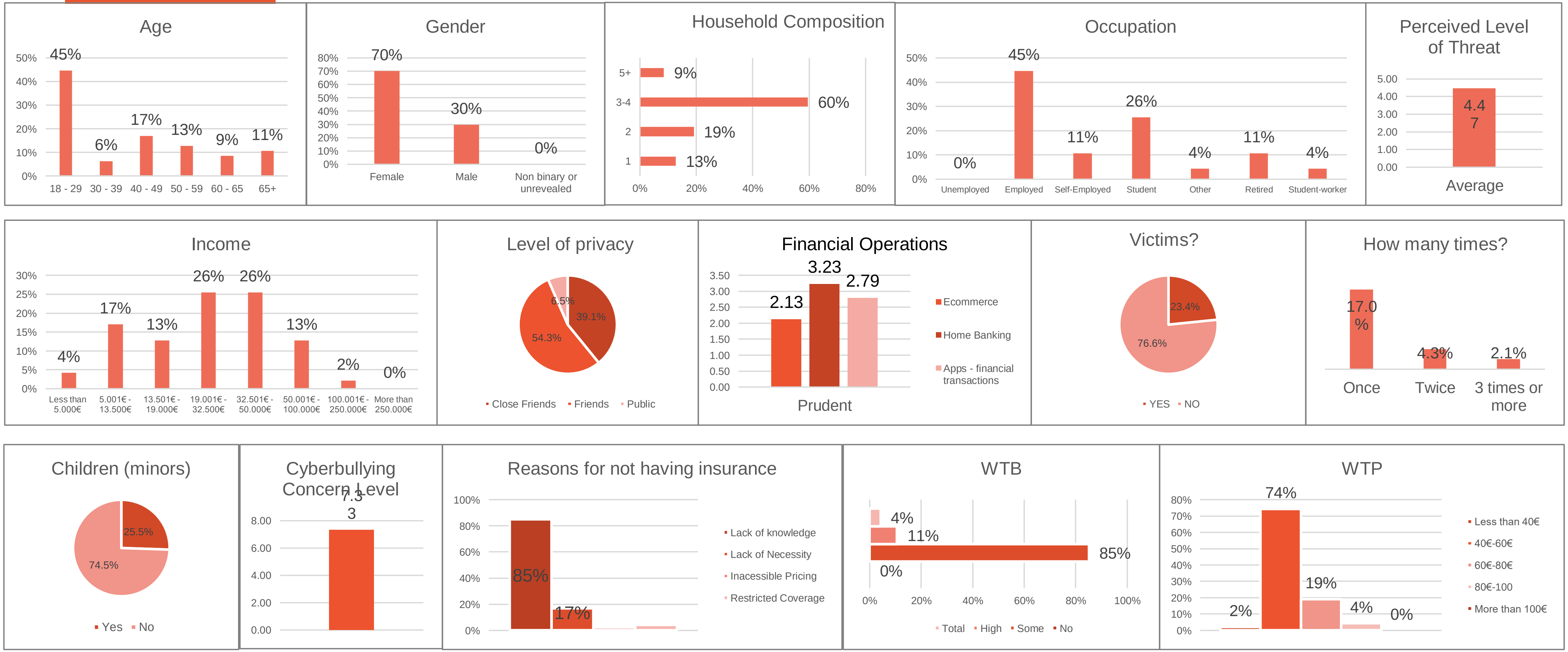
# APPENDIX 19 – PROFILING CLUSTERS (B2C)

## CHANCE TAKER



# APPENDIX 19 – PROFILING CLUSTERS (B2C)

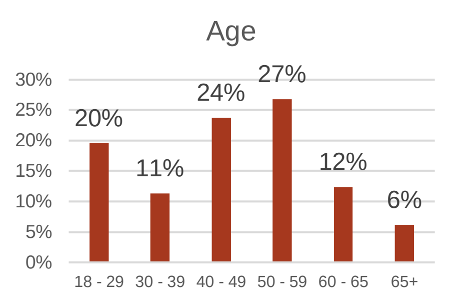
## PRUDENT

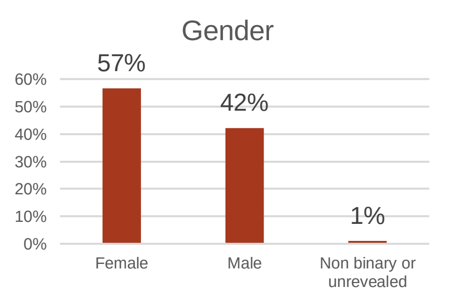


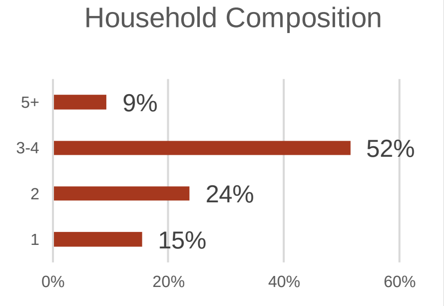
# APPENDIX 19 – PROFILING CLUSTERS (B2C)

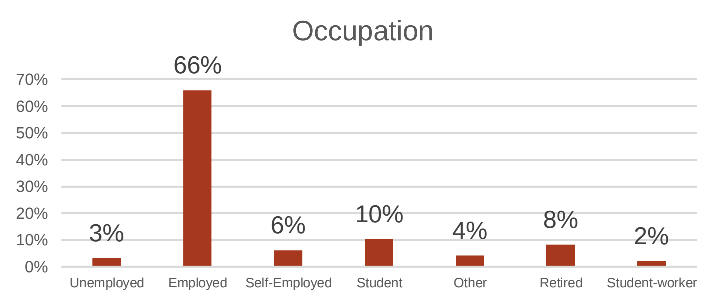
Back to Presentation

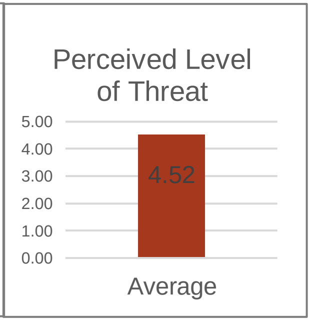
**ALERT**

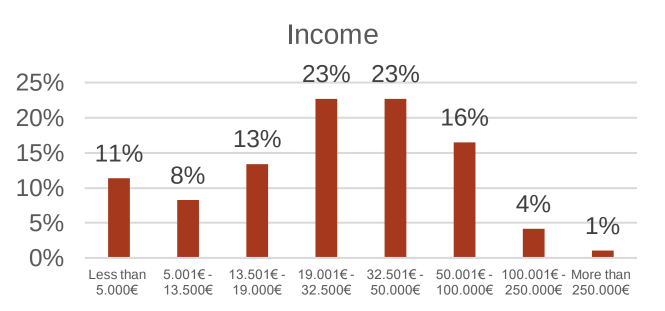


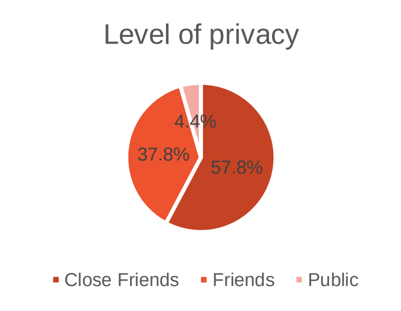



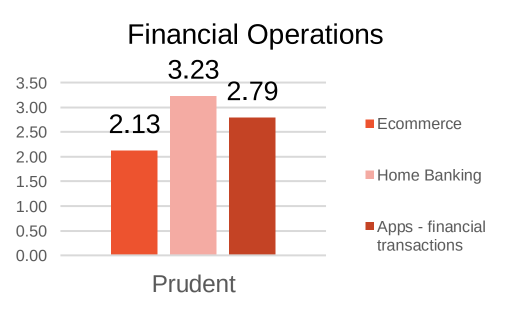



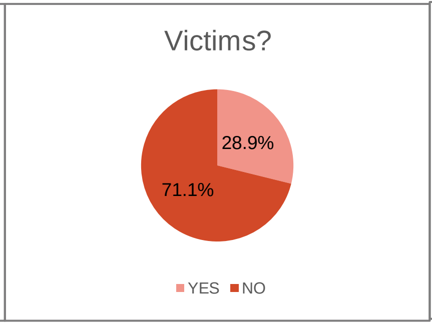



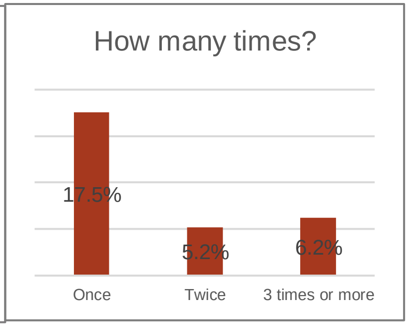



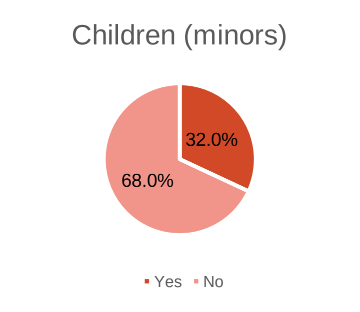



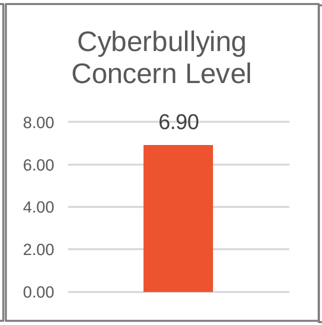



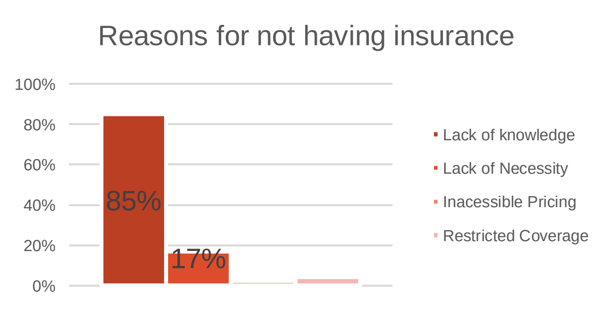



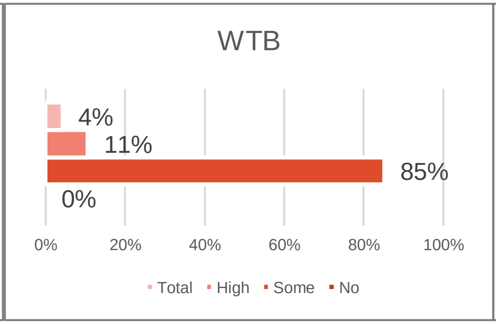



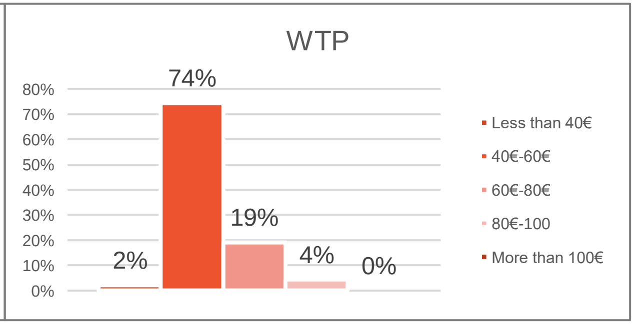



## Agenda

2 **Create customer segments (clusters) according to the calculated variables**

B2C Segment

| Segment Name | EAR | Selection Reasoning |
|---|---|---|
| Ready | + + + | ✔ |
| Miss Independent | + + - | ✔ |
| Big-spender | + - + | ✔ |
| Chance-taker | + - - | ✔ |
| Prudent | - + + | ✔ |
| Alert | - + - | ✔ |
| Misfit | - - + | ✘ |
| Disconnected | - - - | ✘ |

The “Misfit” segment represents people with a low level of tech-savviness and awareness, but high monetary value. We believe this segment does not reflect accurately consumer behavior since, on one hand, it is highly unlikely that people who do not need will buy cyber risk insurance and, on the other hand, the behavior variance within the segment is high.

The ”Disconnected” segment does not represent the ***customer of the future.***

## Agenda

# APPENDIX 21 – CUSTOMER PERSONAS (B2C)

## READY

High Tech
High Awareness
High Monetary Value

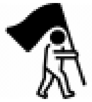
| Age | Level of IT Dependency | Income |
|---|---|---|
| Average<br>**31** | High<br>(8.04/10) | Medium<br>(€36.5K - average) |

**Main Insights**

- Frequent usage of social media;
- Low degree of privacy (mostly public accounts);
- 23% of this segment suffered a cyber attack;
- Almost 50% of this segment pays for online protection.

| WTB | WTP |
|---|---|
| High | High |

## MISS INDEPENDENT



High Tech
High Awareness
Low Monetary Value

| Age | Level of IT Dependency | Income |
|---|---|---|
| Average<br>**38** | High<br>(8.05/10) | Medium (€32K -average) |

**Main Insights**

- Weekly sharing of personal content on social media;
- 2# segment in parents;
- 39% has already been a victim;
- 1# in cyberbullying concern;
- 90% have free or paid online protection;
- Segment claiming the lower necessity for cyber insurance.

| WTB | WTP |
|---|---|
| Medium | Low |

**Sources**: *Surveys*

## BIG SPENDER

**High Tech**
**Low Awareness**
**High Monetary Value**

| Age | Level of IT Dependency | Income |
|---|---|---|
| Average<br>**28**<br>(youngest segment) | High<br>(8.12/10) | High (€75K – average) |

### Main Insights

- Segment with the lower number of parents;
- Almost 50% are students;
- #1 in risky behaviors;
- Frequent usage of social media;
- Low degree of privacy (mainly public accounts);
- 50% of the victims in this segment had more than 3 incidents.

| WTB | WTP |
|---|---|
| **High** | **High** |

## CHANCE TAKER

**High Tech**
**Low Awareness**
**Low Monetary Value**

| Age | Level of IT Dependency | Income |
|---|---|---|
| Average<br>**31** | High<br>(8.05/10) | Medium (€32K -average) |

### Main Insights

- Almost 50% of the segment is composed of students;
- Frequent usage of social media;
- Low postage on social media;
- 67% do not know the level of online protection of their children;
- Only 3% of this segment has suffered cyber attacks.

| WTB | WTP |
|---|---|
| **Low** | **Low** |

***Sources**: Surveys*

# APPENDIX 21 – CUSTOMER PERSONAS (B2C)

Back to Presentation

## PRUDENT

Low Tech
High Awareness
High Monetary Value

| Age | Level of IT Dependency | Income |
|---|---|---|
| Average<br>**40** | Low<br>(5.82/10 | Medium (€34K - average) |

**Main Insights**

- #1 in retired people;
- #1 in fewer risk behaviors;
- High level of privacy (mostly private profiles);
- Segment that prioritizes the most children's online protection (2# in concern regarding cyberbullying)
- 90% have free or paid online protection;
- 83% monitor their children's activities online.

| WTB | WTP |
|---|---|
| Low | Medium |

## ALERT

Low Tech
High Awareness
Low Monetary Value

| Age | Level of IT Dependency | Income |
|---|---|---|
| Average<br>**46**<br>(oldest sector) | Medium<br>(6.59/10) | High (64K – average) |

**Main Insights**

- Segment with the highest number of parents;
- #1 in prioritizing their kids' online protection over theirs;
- #2 in fewer risk behaviors;
- High level of privacy on social media;
- 29% of this segment has been a victim;
- More than 90% have free or paid online protection.

| WTB | WTP |
|---|---|
| Low | Low |

## Agenda

# APPENDIX 22 – PRODUCT FEATURES (B2B)

## Comparison of CyberShield and Competition

### Pre-Breach

| | | | | |
|---|---|---|---|---|
| **RISK ASSESSMENT** | | | | |
| Risk Diagnosis | ● | ● | ● | ● |
| Regulatory Compliance Evaluation | | ● | ● | ● |
| **RISK MITIGATION** | | | | |
| Network Security | | ● | ● | ● |
| Access Control | | ● | ● | ● |
| Employee Education → **Beyond Insurance** | | | | ● |
| **RISK MONITORING** | | | | |
| Continuous Risk Assessment & Mitigation | | ● | ● | ● |
| Contingency Plan | | ● | ● | ● |

Legend:
- Ageas (New Product)
- Ageas (Product under development)
- Main Players (Fidelidade, Tranquilidade, Allianz)
- Other Players (Caravela, Visavis, MDS, Innovarisk, AIG)

### Post-Breach

| | | | | |
|---|---|---|---|---|
| **1st PARTY** | | | | |
| Business Interruption | ● | ● | ● | ● |
| Extortion | ● | ● | ● | ● |
| Data & Software Reconstitution | ● | ● | ● | ● |
| Regulatory Fines & Sanctions | ● | ● | ● | ● |
| **3rd PARTY** | | | | |
| Liability | ● | ● | ● | ● |
| **OTHER BENEFITS** | | | | |
| Forensic Investigation | ● | ● | ● | ● |
| Legal Advice & Defense | ● | ● | ● | ● |
| Credit/Identity Monitoring | ● | ● | ● | ● |
| Notifications | ● | ● | ● | ● |
| Communication | ● | ● | ● | ● |

***Sources**: Ageas, Fidelidade, Tranquilidade, Allianz, Caravela, Innovarisk, Visavis, MDS, AIG*

## Value Proposition - SMEs

### General Cyber Insurance Coverage Components

**Benchmarking evidence shows that on average, all players offer:**

**PROPOSED TAXONOMY[1]**

**1st Party**
Coverage against direct losses incurred by the insured, mostly consisting of business interruption and costs associated with mitigating a cybersecurity event.

**3rd Party**
Liability coverage indemnifying companies for losses to others.

**Other Benefits**
Related to assorted costs and services.

+

### Pre-breach Services

**Major players offer:**

**Risk Assessment**
Evaluation of vulnerabilities

**Risk Mitigation**
Preparation & Prevention

**Risk Monitoring**
Continuous assessment & contingency plans

### AGEAS WILL DIFFERENTIATE IN BEYOND INSURANCE THROUGH TARGETED EMPLOYEE TRAINING

**REVOLUTIONARY HUMAN RISK MANAGEMENT PLATFORM (SAAS)**

*"Go beyond security awareness training to visualize risk, target interventions, and prevent data breaches like never before. This is predictive human risk intelligence."*

OutThink


### WHY GO "BEYOND INSURANCE"?

"*Cyber insurance will always complement the essential service - risk mitigation.*" (Bruno Soares, IDC)

**REDUCED NUMBER OF CLAIMS**

Mitigating risk allows for a higher level of prevention and protection, decreasing the number of potential claims and, thus, lower loss ratios.

**MAIN PLAYERS ARE INCLUDING PRE-BREACH SERVICES**

Benchmarking evidence has proven this assumption.

**INTEGRATED & COMPREHENSIVE CYBERSECURITY APPROACH**

SMEs have limited resources and aim to centralize cybersecurity to consolidate the threat cycle. Thus, an offer that allows not only risk transferring, but also assistance and possibly beyond is ideal.

**AGEAS MISSION & PURPOSE**

Going the extra mile and offering a product that allows for an ongoing relationship with the client is fully aligned with Ageas mission of delivering an "emotional and meaningful experience".

[1]*ENISA Framework* | ***Sources**: Ageas Portugal, Benchmarking Evidence, ENISA, Industry Expert Interviews, OutThink*

## Agenda

# APPENDIX 23 – PRODUCT FEATURES (B2C)

## Comparison of CyberShield and Competition

### Pre-Breach

**RISK MITIGATION**

| | | | |
|---|---|---|---|
| Identity Access Management | ● | | ● |
| Back-up System Configuration | | ● | ● |
| Network Security | | | ● |

**RISK MONITORING**

| | | | |
|---|---|---|---|
| Continuous Risk Assessment & Mitigation | | | ● |
| Parental Control | | ● | ● |

### Post-Breach

**LEGAL COVERAGE**

| | | | |
|---|---|---|---|
| Violations of Personal Privacy | ● | ● | ● |
| Online Shopping | ● | ● | ● |
| Online Accounts & Credit Cards | ● | ● | ● |
| Legal Advice & Defense | | ● | ● |

**ASSISTANCE COVERAGE**

| | | | |
|---|---|---|---|
| Software Repairing | | ● | ● |
| File Loss Reconstitution | | ● | ● |
| Psychological Counselling | | ● | ● |
| Tracking/Deleting Sensitive Information | ● | ● | ● |
| Devices Geolocation & Block | | ● | ● |
| Technical Assistance | | ● | ● |

Legend:
- ● Ageas
- ● Fidelidade
- ● Inter Partner Assistance

***Sources**: Fidelidade, Inter Partner Assistance*

## Value Proposition - Families

### General Cyber Insurance Coverage Components

**Benchmarking evidence shows that, on average, all players offer:**

**Legal Coverage**
Coverage against legal expenses which are filed within the scope of personal life, due to an act practiced through the internet, social networks, or any other electronic means of communication.

**Assistance Coverage**
Coverage and post-breach assistance provided in consequence of a claim, including software and data restoring, counselling, and technical assistance.

**No player currently offers comprehensive pre-breach services:**

**Risk Assessment**
Evaluation of vulnerabilities

**Risk Mitigation**
Preparation & Prevention

**Risk Monitoring**
Continuous assessment

### AGEAS WILL DIFFERENTIATE BY GOING BEYOND INSURANCE AND OFFERING PRE-BREACH SERVICES

**Risk assessment and mitigation services:** Norton

"To help safeguard consumers in today's evolving digital universe, NortonLifeLock has evolved to provide all-in-one protection. Around the globe in more than 50 countries, people and families rely on NortonLifeLock products to help protect against viruses, malware, online tracking, attacks on home Wi-Fi networks, identity theft, plus much more."

**Main features:**
- Protection against spyware, virus, malware and ransomware
- Back-up in cloud for PC
- Password manager
- Parental control


**WHY GO "BEYOND INSURANCE"?**

*"Cyber insurance will always complement the essential service - risk mitigation."* (Bruno Soares, IDC)

**REDUCED NUMBER OF CLAIMS**
Mitigating risk allows for a higher level of prevention and protection, decreasing the number of potential claims and, thus, lower loss ratios.

**INTEGRATED CYBERSECURITY APPROACH**
Individuals and families aim to centralize cybersecurity to consolidate the threat cycle. Thus, an offer that allows not only risk transferring, but also assistance and possibly beyond is ideal.

**AGEAS MISSION & PURPOSE**
Going the extra mile and offering a product that allows for an ongoing relationship with the client is fully aligned with Ageas mission of delivering an "emotional and meaningful experience".

***Sources**: Norton*

## Agenda

## Pre-breach Services: Description, Exclusion and Limits (SMEs)

| Features | Description & Definitions | Exclusions | Sub-limits |
|---|---|---|---|
| **Vulnerability Analysis & Resolution** | Analysis of the vulnerabilities of its public IP, as well as of the devices connected to the Internet, to detect patent vulnerabilities and open communication ports.<br>The service will be performed through a fully automated application, allowing the Company to identify the vulnerabilities classified by severity:<br>• Critical: very easily exploited a vulnerability that can put the Computer Device at risk as well as the data contained therein;<br>• High: easy to exploit a vulnerability that could put the Computer Device and the data on it at risk contained;<br>• Medium: complex exploitation vulnerability, which could allow the blocking of the Computer Device and the information theft;<br>• Low: a vulnerability that is difficult to exploit and that in itself does not imply a risk, but that, combined with others may involve risks;<br>• Informational: information available from the Computer Device, which, without causing risks, can detect exploitable vulnerabilities.<br>Once the analysis has been carried out, the Company will have access to a remote platform to resolve the detected vulnerabilities.<br>In case of critical or high vulnerabilities, a technician will proactively contact the insured. | Fidelidade:<br>The following are not included in the Services Provided:<br>- Updates and/or software installations that involve additional expenses;<br>- The management and/or updates of software used by the Insured without having the necessary licenses in force;<br>- Updates that cannot be made by remote assistance by the Insurer;<br>- Regarding systems, devices, and information for the Insured's and the Insured's employees' personal use. | Unlimited access to the platform - available 365 days per year |
| **Web Vulnerability Research** | Exhaustive test of the vulnerabilities of common Web applications, such as SQL Injection, cross-site scripting (XXS), HTTP header, remote file inclusion directory and execution of commands.<br>In case of critical vulnerabilities, a technician may proactively contact the Insured for its resolution. | | Unlimited access to the platform - available 365 days per year |
| **Safety Manual – Recommendations** | Recommendations Manual: The Insured shall be provided with a recommendations guide which it shall implement to be protected against cyber attacks. The recommendations include the following prevention policies:<br>• Recommendations on how to act against information hijacking;<br>• Steps that must be taken for correct configuration of connected programs and devices;<br>• Plan the appropriate password policy for your Insured;<br>• Recommendations on mobile devices;<br>• Policy with employees;<br>• Confidentiality; Recommendations and safety manual. | | 1 manual per policy and per year |

## Pre-breach Services: Description, Exclusion and Limits (SMEs)

| Features | Description & Definitions | Exclusions | Sub-limits |
|---|---|---|---|
| **GDPR Compliance Evaluation and Guide** | Access to a web portal to self-assess the degree of compliance with the GDPR. By means of a self test, a report - provided in electronic format - is immediately generated with the degree of compliance of the company and, if necessary:<br>- information to guide it to comply with the provisions of the GDPR;<br>- possible sanctions that the company may incur in case of non-compliance. | | - Unlimited access to the web portal<br>- 1 implementation guide |
| **Back-up System And Encryption Configuration** | 1. Configuration of restoration systems (Back-up/Shadow Copy, VSS, or others)<br>2. The Back-up service in the "Cloud" provides the Insured with a secure storage environment to be able to make back-up copies, store or share information in a secure manner.<br>Through remote assistance, the Insured has the possibility to configure a back-up system with the following characteristics:<br>• Back-up copies of the essential data for the Insured's operation. Automatic, easy-to-use online copies for PCs and Macs. Capacity according to the size of the Insured (512G up to 3 employees, 1 Tera up to 10 employees, 1.5T up to 20 employees, and 2T up to 50 employees);<br>• Possibility of access to files, not only from the computer but also from Android and IOS applications;<br>• Automatic and continuous protection. Whenever connected to the Internet, the data will be encrypted and transmitted automatically and stored in several data centers with 24-hour surveillance;<br>• AES-256 military-grade encryption;<br>• When changing a file, it will also be changed automatically in its copy in the "cloud";<br>• 30 previous versions of each of your files are saved;<br>• Each deleted file will be kept for 30 days. | Must have configured the back-up recovery system in the Cloud for the "disaster recovery plan" to work.<br><br>The following are not included in the Services Provided:<br>- Updates and/or software installations that involve additional expenses;<br>- The management and/or updates of software used by the Insured without having the necessary licenses in force;<br>- Updates that cannot be made by remote assistance by the Insurer;<br>- Regarding systems, devices, and information for the Insured's and the Insured's employees' personal use | Unlimited access to the platform - available 365 days per year |

## Pre-breach Services: Description, Exclusion and Limits (SMEs)

| Features | Description & Definitions | Exclusions | Sub-limits |
|---|---|---|---|
| **Network Security** | • **Update** of Computer Devices keeping installed the **latest patches** of the Operating System; Installation of Standard Applications, whenever the respective license is available.<br>• Verification and configuration of **anti-virus.**<br>• Secure configuration of the company's **Wi-Fi network.**<br>• Verification and configuration of the system's **firewalls.**<br>• Verification of the **output connections** of the computer system. | 1. Assistance will be provided through a dialogue tool, like chat, which will allow the Company to contact with specialized technicians.<br>2. Through the computer platform available on the Internet, the Insured will be able to access the remote assistance service and secure configuration of their systems. The service allows for the review of the computer system, as well as the detection/removal of malware, temporary files, cookies and services that delay or endanger the security of data or the operation of the Insured's computers covered by the policy.<br>3. During the provision of the service, specialized technicians may assume the control of the computer devices, provided that it is previously authorized by the Insured and always under supervision.<br>4. In case the Insured does not have access to the Internet, it will have at his disposal a telephone computer assistance service, which allows queries related to security incidents, as well as advice to adopt security measures in: systems, computers, servers, laptops, tablets, smartphones; | 1 implementation by policy and per year |
| **Control Recovery of Pirated Accounts** | Providing advice to the Insured if their accounts have been hacked because they have been victims of password theft or identity theft. If offensive messages were sent from the hacked account, or inappropriate photographs were uploaded, false content was posted on behalf of the account holder, the service helps the affected person to recover his/her pirated account.<br>The access passwords will be changed and the published content will be deleted without your permission. | Must have configured the back-up recovery system in the Cloud for the “disaster recovery plan” to work.<br><br>The following are not included in the Services Provided:<br>- Updates and/or software installations that involve additional expenses;<br>- The management and/or updates of software used by the Insured without having the necessary licenses in force;<br>- Updates that cannot be made by remote assistance by the Insurer;<br>- Regarding systems, devices, and information for the Insured's and the Insured's employees' personal use | 1 recovery per policy and per year |

Back to Presentation

## Pre-breach Services: Description, Exclusion and Limits (SMEs)

| Features | Description & Definitions | Exclusions | Sub-limits |
|---|---|---|---|
| **Anti-hijacking App** | An Anti-hijacking application that allows you to detect and block ransomware, i.e. malware that can infect your computer devices, encrypting the system's data (documents with more common extensions, such as .doc, .xls, .pdf, etc.).<br>**App Features:**<br>• Prevents ransomware, the encryption of data and execution of programs with names of extensions and locations normally used by the ransomware;<br>• Designed to prevent infection by ransomware by configuring operating system rules and monitoring suspicious activity on files;<br>• Once suspicious activity is detected, the malicious process is identified and immediately blocked, with a warning displayed on the affected computer's screen.<br>• If necessary, remote assistance from a specialized technician will be available to the company to carry out the installation. | | Devices per policy and per year:<br>- Plan Base: 10<br>- Plan Plus: 50<br>- Plan Total: 100<br>- Plan Extra: 250 |
| **Employee Targeted Training**<br><br>(Partnership with UK's Start-up OutThink) | **Visualize risk – the complete picture:**<br>1) Measure & understand the company's human risk;<br>2) Identify high-risk departments<br>3) Identify high-risk employees<br><br>**Targeted interventions (training) – predictive human risk intelligence:**<br>1) Suggested actions from department to employee: OutThink will provide both automated and manual targeted interventions from historically proven risk treatment methods from the company level to the individual.<br>2) Measure impact and escalate interventions: See your organization's human risk profile change in real-time and investigate further if security behaviors do not improve.<br>3) Learn what works and apply across the organization: Track improvements and continue to deliver proven targeted interventions across the company. | | Employees per policy and per year:<br>- Plan Base: 10<br>- Plan Plus: 50<br>- Plan Total: 100<br>- Plan Extra: 250 |

## Agenda

## Employee Security Awareness Training: Potential Partners (I/II)

**Category:** Security Awareness Computer-Based Training Market


Figure 1. Magic Quadrant for Security Awareness Computer-Based Training


Source: Gartner (November 2018)

| Partners | Location | Description | Garner Rating (Scale 1-5) |
|---|---|---|---|
| OutThink | United Kingdom | ***OutThink Human Risk Management Platform (SaaS)*** *"OutThink is a revolutionary Human Risk Management Platform (SaaS) empowering CISOs by targeting the source of 90% of all data breaches: human behavior."* | 5.0★ |
| IRONSCALES | Israel | **IronScales Awareness and Training** *"Cloud-based anti-phishing platform that provides businesses with a complete solution for enterprise email security.* | 5.0★ |
| KnowBe4 Human error. Conquered. | United States | **Enterprise Awareness Training Program** *"Comprehensive new-school approach that integrates baseline testing using mock attacks, engaging interactive web-based training, and continuous assessment through simulated phishing, vishing, and smishing attacks to build a more resilient and secure organization."* | 4.7★ |

***Sources**: Gartner, OutThink, IronScales, KnowBe4*

# APPENDIX 25 – EMPLOYEE TRAINING: POTENTIAL PARTNERS (B2B)

Back to Presentation

## Employee Security Awareness Training: Potential Partners (I/II)

**Category:** Security Awareness Computer-Based Training Market


Figure 1. Magic Quadrant for Security Awareness Computer-Based Training


Source: Gartner (November 2018)

| Partners | Location | Description | Garner Rating (Scale 1-5) |
|---|---|---|---|
| TERRANOVA SECURITY | Canada | **Terranova Security Awareness Platform** *"Target, evaluate, and track your security awareness campaigns."* | 4.7 ★ |
| Barracuda | United Kingdom | **Barracuda PhishLine** *"Gives you the option to create a completely customized program or opt for the Quick Launch process to get an awareness campaign up and running in under a minute. Quick Launch simplifies security awareness with an easy 5-step click-thru setup, proven curated testing and training content, and efficient, automated reports."* | 4.5 ★ |
| SOPHOS | United Kingdom | ***Sophos Phish Threat*** *"Educates and tests your end users through automated attack simulations, quality security awareness training, and actionable reporting metrics."* | 4.3 ★ |

***Sources**: Gartner, Terranova, Barracuda, Sophos*

## Agenda

## Post-breach Services (1st party): Description, Exclusion and Limits (SMEs)

| Coverage | Description & Definitions | Requisites | Exclusions | Sub-limits |
|---|---|---|---|---|
| **Business Interruption: Loss of Income Extra Expenses** | **Business Interruption:** The interruption (total or partial) is a direct and exclusive consequence of an incident in the company's computer system entity.<br><br>**Calculation of reduction in net income:** The Insurer will pay the difference between the actual net result (profit or loss) obtained during the indemnity period and the net result (profit or loss) that the entity would have obtained in the same period of the previous year or if in the first year of activity, the difference between the compensation period and the period immediately prior to the interruption.<br>• Grace Period: loss of income coverage has no effect;<br>• Indemnity Period: Period of time elapsed from the date of the alert to the assistance service participating in the interruption, until the resolution of the incident by the Insurer, in a maximum of 30 days.<br><br>**Extra Expenses:** Fixed operating costs (including salaries).<br>Expenses to mitigate the loss of profits:<br>• Rental of computer equipment;<br>• Fees of an external provide;<br>• Technological computer forensics to contain the incident;<br>• The increase in the entity's labor cost. | The first 24 h since the first notification to the assistance service shall be considered as grace period*<br><br>Expenses < potential reduction in the net result (previous written consent of the Insured) | 1. Losses resulting from the suspension/cancellation of any contract, licenses, or orders.<br>2. Penalties (e.g. delay in deliveries)<br>3. Scheduled maintenance, longer than expected (including a system slowdown)<br>4. Insured's computer system fails to respond to the operating situation by not anticipating or plan the referred unless the problem is the result of a cyber attack.<br>5. Arising from programs/systems used by the Insured without necessary permits in force.<br>6. Costs arising from an infringement of IP rights. | 25% of insured capital, at most €75.000 |

## Post-breach Services (1st party): Description, Exclusion and Limits (SMEs)

| Coverage | Description & Definitions | Requisites | Exclusions | Sub-limits |
|---|---|---|---|---|
| **Cyber Extortion (Ransomware)** | Fees and other expenses incurred by an expert consultant or by the entity to assist the insured in responding to the threat of extortion - eliminate or mitigate extortion damages (attempted or consummated manner)<br><br><u>Cyber Extortion (Ransomware):</u> One credible threat, or a series of credible threats linked together, made by someone who is not familiar, to an employee, member of a corporate body, responsible, shareholder or partner of the Insured, to cyberattack the Insured. | 1. Inform (and update) immediately the Insurer of the threat.<br>2. The Insurer has given its prior written consent to any payment.<br>3. Submit proof of the amounts spent and demonstrate that every effort was made to avoid it (prove that the threat was real and not fictitious)<br>4. A director (or equivalent position) has given his consent to the payment<br>5. Notify the threat to the police or the other authority.<br>6. The Insurer's Technical Services have considered that technically the payment of the "Rescue" is a more viable alternative than recovery of data covered in the policy.<br>7. The Insured maintains strict secrecy about the existence and terms of this coverage. | It is not legally permissible to pay extortion cybernetics by the Insured or Insurer in the face of current legislation. | General attack on several entities: 5% of insured capital, at most €15.000<br><br>Specific attack on the Insured's network: 25% of insured capital, at most €75.000 |

## Post-breach Services (1st & 3rd party): Description, Exclusion and Limits (SMEs)

| Coverage | Description & Definitions | Requisites | • Exclusions | Sub-limits |
|---|---|---|---|---|
| **Data and Software Reconstitution** | Damages caused by viruses/malware:<br>1) Disinfection of viruses<br>2) Recover access to programs or electronic data<br>3) Reconfigure/install from back-ups/other sources<br>4) Replace a 3rd party program in the entity's computer system | Recoveries cannot have been handled prior to its deliver to the specialized technician for recovery | 1. Resulting from data exposure not in the custody/control of the Insured, such as data delivered/supported by a "cloud computing" service or data or web pages hosted on servers of a third party (hosting services), except for back-up services arising from the contractor in the policy;<br>2. The recovery of originals, films, CDs, games and other apps.<br>3. Complex storage systems (RAID and physical volume groups), storage servers apps, back-up tapes and web servers.<br>4. Expenses for identifying/correcting vulnerabilities in the computer system<br>5. Expenditure on the development of new programs/electronic data.<br>6. Resulting from non-compliance with data protection regulations<br>7. Occurred in systems, devices and info of the insured's personal use<br>8. Taxes, fines or penalties. | Virus Disinfection/System Restore: 5% per claim, 10% per year (of insured capital), at most €75.000<br><br>Data and Software Restoration: 25% of insured capital, at most €75.000<br><br>1 recovery per policy and per year |
| **Regulatory Fines and Sanctions** | Fines or penalties arising from complaints from administrative proceedings:<br>1. Sanctions imposed by National Data Protection Commission (or equivalent supervisory authority)<br>2. PCI Sanctions; | | 1. Costs derived from the violation of intellectual property, patents, royalties, copyright, trademark and copyright;<br>2. No coverage for fines of a disciplinary, administrative and criminal nature, and / or those that, by law, cannot be covered by insurance;<br>3. Sanctions arising from use of personal data without consent in actions and advertising campaigns. | 100% of insured capital |
| **Liabilities** | Payment of indemnities that the Insured is legally obliged to pay for damages and losses caused to 3rd parties or employees for malicious or unauthorized use of the Insured's computer network with the intent to cause:<br>1) Damage, alteration, corruption, distortion, unauthorized copying, error, theft, misuse, or destruction of 3rd party digital assets/data;<br>2) Denial of service to third parties;<br>3) Acts of "Phishing", "Pharming" or any kind of misleading communication to obtain confidential data or information from 3rd parties;<br>4) Transmission of malicious code; | | 1. Actual/assumed error in the info or description of prices and the authenticity of g&s.<br>2. Incorrect or incomplete estimate, info or guarantee regarding prices and costs;<br>3. Total or partial description of goods, products and services related to their quality or performance;<br>4. Real, alleged or assumed error in the financial information disclosed or published by the or on behalf of the Insured;<br>5. All types of games, lotteries, contests and promotional activities or games or other games of chance;<br>6. Fines and penalties of a criminal nature, not insurable by law or that can be imposed directly the external service provider;<br>7. Loss, compensation or reimbursement of fees, commissions, royalties, gratuities or benefits by the Insured, or the costs of providing new services.<br>8. Costs of complying with any instruction, judgment or agreement to offer compensation or any other type of refund that is not economic; | 100% of Insured Capital |

## Post-breach Services (Other Benefits): Description, Exclusion and Limits (SMEs)

| Coverage | Description & Definitions | Requisites | Exclusions | Sub-limits |
|---|---|---|---|---|
| **Forensic Investigation** | Reasonable and necessary expenses of IT experts to:<br>• Finding evidence of the attack;<br>• Damage identification;<br>• Investigation of the case;<br>• Activity identification;<br>• Identification of affected records;<br>• Incidence summary report. | Expenses incurred by the Insured must always comply with reasonability criteria and require prior written authorization from the Insurer. | No expenses with services or work provided by professionals indicated by the Insured are guaranteed. | 25% of Insured Capital, at most €75.000 |
| **Legal Advice and Defence** | 1. Choose a lawyer to represent the company's interest in legal matters;<br>2. Court fees, expenses preparation, court fees in judicial and arbitration proceedings (until capital limit set in General Conditions);<br>3. Other reasonable expenses necessary to defend the Insured (e.g. investigation and expert reports);<br>4. Constitution of bails or judicial guarantees that are required of the Insured to guarantee civil liability;<br>5. Right to arbitrage in case of conflict between insurer and insured | | 1. Fines and other charges of fiscal nature;<br>2. Attorney fees and court costs concerning actions proposed by the Insured without the prior agreement of the Insurer or the Management Entity;<br>3. Benefits that have not been requested from the Insurer or the Management Entity and that have been carried out without agreement, except in cases of force majeure or demonstrated material impossibility.<br>The Insurer and the Management Entity are not obliged to bear the expenses resulting from a lawsuit, when:<br>• Consider, in advance, that it does not have sufficient probabilities of success;<br>• The third party responsible is unknown;<br>• The responsible third-party is insolvent;<br>• The compensation proposal presented by the responsible third party is considered to be fair and sufficient;<br>• The amount corresponding to the disputed interests is less than €X | 100% of insured Capital |
| **Notification** | 1. Expenditure on notifying any regulatory authority about the violation of data, whenever the insured is legally obliged to do so.<br>2. Expenses for using an external call centre (“call centre”), to respond to previously reported issues of injured parties because of a data breach.<br>3. Expenditure on notifying those injured by the data breach. | Expenses incurred by the Insured must always comply with reasonability criteria and require prior written authorization from the Insurer.<br>72 Hours to notify the injured of the data breach | There is no guarantee of any expenses with public relations services or work performed by professionals appointed by the Insured. | 25% of Insured Capital, at most €75.000 |

# APPENDIX 26 – REQUISITES, EXCLUSIONS, LIMITS (POST-BREACH – B2B)

## Post-breach Services (Other Benefits): Description, Exclusion and Limits (SMEs)

| Coverage | Description & Definitions | Requisites | Exclusions | Sub-limits |
|---|---|---|---|---|
| **Credit/Identity Monitoring** | The expenses incurred by the Insured in the provision of banking data control and monitoring services and/or assistance in case of illicit appropriation of identity affecting third parties or employees of the Insured. | Expenses incurred by the Insured must always comply with reasonability criteria and require prior written authorization from the Insurer. | | 25% of Insured Capital, at most €75.000 |
| **Communication** | Costs reasonably incurred by the Insured with a Public Relations specialist or companies specialized in crisis management in the media, to protect or restore the Insured's public image and reputation following malicious or unauthorized use of the computer network of the Insured with damage to third parties | Only the expenses incurred by the insured during the 14 days following the first news or public disclosure of the harmful event will be considered<br>Expenses incurred by the Insured must always comply with reasonability criteria and require prior written authorization from the Insurer. | No expenses with services or work provided by professionals indicated by the Insured are guaranteed | 25% of Insured Capital, at most 75.000.€ |

## Agenda

# APPENDIX 27 – POTENTIAL ONLINE PROTECTION PROVIDERS (B2C)

Back to Presentation

## Online protection (with parental control): Potential providers

| Online Protection Providers | **Selection Reasoning –** Online multi-device protection including parental control | | Price (1 year) |
|---|---|---|---|
| Norton LifeLock | • Protection (spyware, virus, malware ransomware)<br>• Firewall and secure VPN<br>• Back-up in the cloud for PC<br>• Secure VPN and Firewall<br>• Password manager<br>• Parental control | Norton 360 Deluxe – 5 devices | €34,99 (~~€94,99~~) |
| | | Norton 360 Premium – 10 Devices | €39,99 (~~€104,99~~) |
| Bitdefender | • Threat detection<br>• Performance optimization<br>• Parental control<br>• Multilayer protection against ransomware<br>• Secure VPN | Bitdefender FAMILY PACK – 15 Devices | €44,99 (~~€99,99~~) |
| kaspersky | • Protection (spyware, virus, malware ransomware)<br>• Performance optimization<br>• Extra security layer - online banking/shopping<br>• Password manager<br>• Safe Kids (Parental control) | Total Security – 3 devices (1 account) | €79,95 |
| | | Total Security – 5 devices (2 account) | €99,95 |
| McAfee | • Anti-virus<br>• Performance Optimization<br>• Domestic networks security<br>• Password Manager<br>• Encrypted Back-up<br>• Parental control | McAfee Family – 10 devices | €49,95 (~~€99,95~~) |

***Sources**: Norton, Bitdefender, Kaspersky, McAfee*

## Agenda

Back to Presentation

## Pre-breach Services (Legal Coverage): Description, Exclusion and Limits (Families)

| | | Description | Exclusions | Sub-limits | |
|---|---|---|---|---|---|
| | | | | Plan Base | Plan More |
| **Identity access management** | | 1. Monitoring of e-mail accounts incl. delivery of warnings if the accounts are affected by a data leak (e.g. data leak in the case of online vendors);<br>2. Support for reactivating e-mail accounts and deleting fake profiles in the case of identity fraud;<br>3. Checking received e-mails for phishing (e.g. verification of the sender and the URL in the e-mail);<br>4. Enforcement of claims against third parties (e.g. credit card providers);<br>5. Assistance and information on the risks, as well as tips on proper behavior on the internet;<br>6. Password management platform. | - | Unlimited | Unlimited |
| **Back-up system configuration** | | 1. Data synchronization between devices and Cloud integration;<br>2. Parameterization of back-ups on devices and respective recovery;<br>3. “Logical” information retrieval. | - | Unlimited | Unlimited |
| **Network Security** | Anti-virus | Verification and configuration of anti-virus. | - | Unlimited | Unlimited |
| | VPN | Secure configuration of the household's Wi-Fi network. | - | Unlimited | Unlimited |
| | Firewalls | Verification and configuration of the household's firewalls. | - | Unlimited | Unlimited |
| **Risk assessment and mitigation dashboard** | | The Insured has access to an initial analysis of the vulnerabilities of the electronic devices connected to the Internet. The service will be performed through a fully automated application, provided by the AV company. Once the analysis has been carried out, the Insured will have access to a remote platform displaying major risk prevented and possible threats. | - | Unlimited | Unlimited |
| **Parental Control** | | Service that provides support in setting reasonable limits to the use of electronic devices by underage users, avoiding access to inappropriate pages, and allowing greater security in navigation. The service may involve installing an application on the devices of minors belonging to the policyholder's household. The Assistance Service will provide telephone technical support for installing the application, as well as for clarifying doubts related to its operation. | Parental control is restricted to the purpose of supervising the use of devices by minors, and its use for adult supervision is prohibited. | Unlimited | Unlimited |

## Agenda

## Post-breach Services (Legal Coverage): Description, Exclusion and Limits (Families)

<table>
<tr><th colspan="2" rowspan="2"></th><th rowspan="2">Description</th><th rowspan="2">Exclusions</th><th colspan="2">Limits</th></tr>
<tr><th>Plan Base</th><th>Plan More</th></tr>
<tr><td rowspan="2">Violations of personal privacy</td><td>Legal protection</td><td>The following services are insured within the scope of the sum insured specified in the policy:<br>The costs of providing legal services with the claim, extrajudicial and judicial, against an identified third party responsible for actions usually designated as cyberbullying, sexting and grooming and, in general, any form of threat, coercion, harassment, identity theft, defamation or injury an act practiced through the internet, social networks or any other electronic means of communication, which does not result from a contractual relationship and that causes moral, bodily, property and non-property damage to the Insured Person.</td><td rowspan="2">The insurance does not cover:<br><u>Violations of personal privacy:</u><br>1. As a consequence of provocation by the insured. This applies even in the case that the insured responded to an earlier provocation from the attacking person;<br>2. In connection with a political or religious activity of the insured;<br>3. In connection with the principal or sideline activity of the insured if this is not expressly indicated in the policy (person of public interest).</td><td rowspan="2">€1500 (per claim) or €3000 (per year)</td><td rowspan="2">€3000 (per claim) or €6000 (per year)</td></tr>
<tr><td>Insured costs</td><td>• Review of claim and assistance with the enforcement of legal claims;<br>• Request, under the threat of legal consequences, to refrain from attacks that violate privacy;<br>• Filing a criminal complaint;<br>• Enforcing claims for removal, injunctive relief, or damages against attackers and website operators in cases that constitute violations of personal privacy;<br>• Mediation between the parties to a dispute.</td></tr>
</table>

# APPENDIX 29 – Exclusions, Limits (Post-breach – B2C)

## Post-breach Services (Legal Coverage): Description, Exclusion and Limits (Families)

| | | Description | Exclusions | Limits | |
|---|---|---|---|---|---|
| | | | | Plan Base | Plan More |
| **Online Shopping** | Legal protection | <u>Insured events:</u><br>• Non-delivery or partial delivery: movable property and downloads that are not delivered 30 days following the expiry of the last communicated delivery date, or are delivered only in part;<br>• Incorrect or defective delivery: movable property that was not delivered as ordered, or not in the agreed condition, or was delivered in a defective condition. The insurance provides coverage for a maximum of 30 days following receipt of the item.<br>• Non-compliance of online purchase contracts in which the insured is a party and recipient of the service, with the following entities:<br>a) Travel agencies;<br>b) Tourism agencies;<br>c) Hospitality;<br>d) Cleaning companies;<br>e) Laundries;<br>f) Dye shops;<br>g) Technical appliance repair services authorized by the manufacturer;<br>h) Moving companies. | Characteristics due to the natural condition of the item do not represent defects (e.g. shading in the case of leather; color and structure in the case of wood products).<br><br>The insurance does not cover:<br>1. Monetary assets;<br>2. Virtual objects (e.g. Property purchased in apps or games);<br>3. Perishable goods, medication and food supplements, weapons, plants, animals, and vehicles that must be registered (motor vehicles, watercraft, and aircraft);<br>4. Movable property that is bought or sold for commercial purposes;<br>5. Damage to items that were bought for resale or commercial/professional use;<br>6. Defects or defective delivery of software programs;<br>7. Consequential damage of any kind.<br>8. Antiques, philatelic or numismatic collections and jewelry or works of art are excluded from the scope of this warranty if their unit value exceeds € 3,000.00 (three thousand euros);<br>9. The purchase and sale of online agreements concluded between individuals. | €1500 (per claim) or €3000 (per year) | €3000 (per claim) or €6000 (per year) |
| | Insured costs | The following services are insured within the scope of the sum insured specified in the policy:<br>• Review of claim and assistance with the enforcement of claims against sellers, buyers and suppliers, as well as against platform operators. | | | |

# APPENDIX 29 – Exclusions, Limits (Post-breach – B2C)

## Post-breach Services (Legal Coverage): Description, Exclusion and Limits (Families)

| | | Description | Exclusions | Limits | |
|---|---|---|---|---|---|
| | | | | Plan Base | Plan More |
| **Online Accounts & Credit Cards** | Legal protection | <u>Insured object:</u><br>•The insurance covers the following privately used items that are the property of the insureds:<br>•Credit, debit, store or SIM cards;<br>•Online accounts (e.g., E-banking, mobile banking such as TWINT, webshops, e-mail accounts, etc.);<br>•Identity and authentication elements (e.g., Login data or identity data and documents).<br><u>Insured events:</u><br>•Illegal acquisition of the insured property and data by third parties (e.g., through skimming, hacking or theft);<br>•Misuse of credit, debit, store or SIM cards;<br>•Misuse of online accounts;<br>•Misuse of identity and authentication elements (identity fraud). | The insurance does not cover:<br>1. Situations originated by the Insured's deliberate actions, gross negligence, negligence, or omission of basic care reasonably required;<br>2. Cryptocurrencies and crypto wallets;<br>3. Losses caused by persons who live in shared accommodation with the insured;<br>4. Losses as a result of the payment of extortion money or due to freely made payments (e.g. in romance scams, grandparent scams, etc.);<br>5. Costs of subscriptions/season tickets and membership fees;<br>6. Costs of losses incurred during use for business purposes. | €1500 (per claim) or €3000 (per year) | €3000 (per claim) or €6000 (per year) |
| | Insured costs | The following services are insured within the sum insured specified in the policy:<br>• Review of claim and assistance with the enforcement of rights concerning erasure or modification of data on the internet;<br>• Review of claim and assistance with the enforcement of claims against third parties and, where necessary, filing charges;<br>• Review of claim and assistance with disputes arising from contracts with Swiss credit card companies in connection with credit card misuse; | | | |

# APPENDIX 29 – Exclusions, Limits (Post-breach – B2C)

## Post-breach Services (Legal Coverage): Description, Exclusion and Limits (Families)

| | Description | Exclusions | Limits | |
|---|---|---|---|---|
| | | | Plan Base | Plan More |
| **Legal advice & defence** | 1. Defense expenses in criminal proceedings, which are filed within the scope of personal life, by an act practiced through the internet, social networks, or any other electronic means of communication, which constitutes the practice of a crime for negligence.<br><br>2. Defence expenses of the Insured Person under the age of 16, in the proceedings brought by facts practiced by them through the internet, social networks or any other electronic means of communication, within the scope of their personal life, and that are typified in law as a crime. | The insurance does not cover:<br>1. Acts that constitute the commission of a crime with intent, serious guilt, or gross negligence;<br>2. Pure negligence or omission of basic care;<br>3. Unable or psychologically ill people;<br>4. Acts practiced in non-credible, in process of insolvency and/or about to be deactivated websites;<br>5. Defence expenses incurred without the permission of the Insurer;<br>6. Defence expenses in disputes between "Insureds" and between them and the Insurer or partners;<br>7. The defense of legal interests resulting from assigned rights, subrogated or arising from joint credits;<br>8. Claims that involve recourse to the judicial system outside Portugal;<br>9. Indemnities, fines, or sanctions in case of a criminal conviction;<br>10. Travel expenses for Insured and witnesses;<br>11. Travel and accommodation expenses presented by the lawyers;<br>12. Expenses that would be incurred by third parties;<br>13. Legal expenses prior to the event;<br>14. All expenses arising from the presentation of documentation to official bodies;<br>15. Expenses arising from an accumulation of claims or judicial counterclaim of matters not included in the contracted guarantees;<br>16. Expenses resulting from events related to damages that already existed at the date of the accident;<br>17. Legal expenses when the claim is not considered viable and the Insured does not reach a proposal for higher compensation or a more favorable outcome for the situation, with the judicial process, or the appeal;<br>18. The amount corresponding to the disputed interests, at the date of the filing of the Action, is less than €120.00. | €1500 (per claim) or €3000 (per year) | €3000 (per claim) or €6000 (per year) |

## Post-breach Services (Assistance Coverage): Description, Exclusion and Limits (Families)

| | | Description | Exclusions | Limits | |
|---|---|---|---|---|---|
| | | | | Plan Base | Plan More |
| **Repairing and/or replacement of lost data and software** | Software repairing | Access to a qualified technician to solve problems that make the Gray Line equipment (desktops, hybrids, laptops, tablets, surfaces, smartphones, scanners, printers) impossible to operate, owned by the Insured Person, at the level operating systems, applications or hardware that prevent their normal and proper use.<br>a) Configuration and parameterization of the installed legal operating systems, as well as the legal software acquired by the Insured Person;<br>b) Troubleshooting the home network, including wireless network range;<br>c) Installation, parameterization, and troubleshooting of computer peripherals;<br>d) Optimization of the operating system and application environment;<br>Insured events<br>• Physical damage to the digital storage medium;<br>• Technical defect in the digital storage medium;<br>• Hacker attacks or infection of a digital storage medium with computer viruses or malware. | 1. Services that have not been requested from the Assistance Service or that have not been made with their agreement;<br>2. Hardware intervention or repair services, including the purchase of parts or components;<br>3. Support services for servers and technological equipment for professional use or collective property;<br>4. The provision of replacement equipment;<br>5. The resolution of problems originating from repeated deficient use or failures to comply with the premises of good use transmitted by the Assistance Service;<br>6. Computer equipment whose operating deficiencies started before the entry into force of this contract. | Non-included | Unlimited |
| | Files loss reconstitution | The insurance covers the following privately used electronic devices that are the property of the insureds:<br>• Virtual clouds (restoration of data from history or back-up);<br>• Storage media and databases (e.g. SSD, NAS, SAN/DAS, RAID).<br><u>Insured events</u><br>• Physical damage to the digital storage medium;<br>• Technical defect in the digital storage medium;<br>• Hacker attacks or infection of a digital storage medium with computer viruses or malware.<br><u>Insured costs</u><br>• Costs of recovering damaged or lost data;<br>• Costs of reinstalling data on devices, databases, or cloud accounts of the insureds; | 1. Physical data recovery services on damaged media; | Non-included | Unlimited |

## Post-breach Services (Assistance Coverage): Description, Exclusion and Limits (Families)

| | Description | Exclusions | Limits | |
|---|---|---|---|---|
| | | | Plan Base | Plan More |
| **Psychological counselling** | 1. In case of threat, coercion, harassment, identity theft, defamation , or injury committed against the Insured Person through the internet, social networks , or any other electronic means of communication, the Assistance Services will provide, by telephone, contact with a Psychologist to advise the "Pessoa Segura";<br>2. This guarantee will be provided by Psychologists with a valid professional card and consultations must be requested at least 24 hours in advance. | 1. This guarantee is only valid if Insurance Plan 2 is contracted and the Legal Protection, Damage Claim guarantee is activated in advance. | Non-included | 4 sessions (per claim) or 8 sessions (per year) |
| **Tracking and deleting sensitive digital information** | Insured Benefits<br>• Monitoring of the internet, as well as publicly accessible online platforms, incl. the delivery of warning messages in the event of defamatory and privacy-infringing content concerning the insureds (e.g. insults, abuse, bullying);<br>• Request to third parties that they cease any further violations of personal privacy and delete the postings concerned;<br>• Request to platform or website operators that they delete privacy-violating postings; | | Unlimited | Unlimited |
| **Devices geolocation and block** | 1. Locate mobile devices in the event of loss or theft, allowing you to block devices remotely or erase your data, avoiding misuse, while also allowing you to control the device 24 hours a day, 7 days a week.<br>2. Technical support for the use of the geolocation and blocking application previously installed as standard on smartphones, both on devices with Android and iOS systems. For this service to work, it is essential to have activated the GPS system. | | Unlimited | Unlimited |

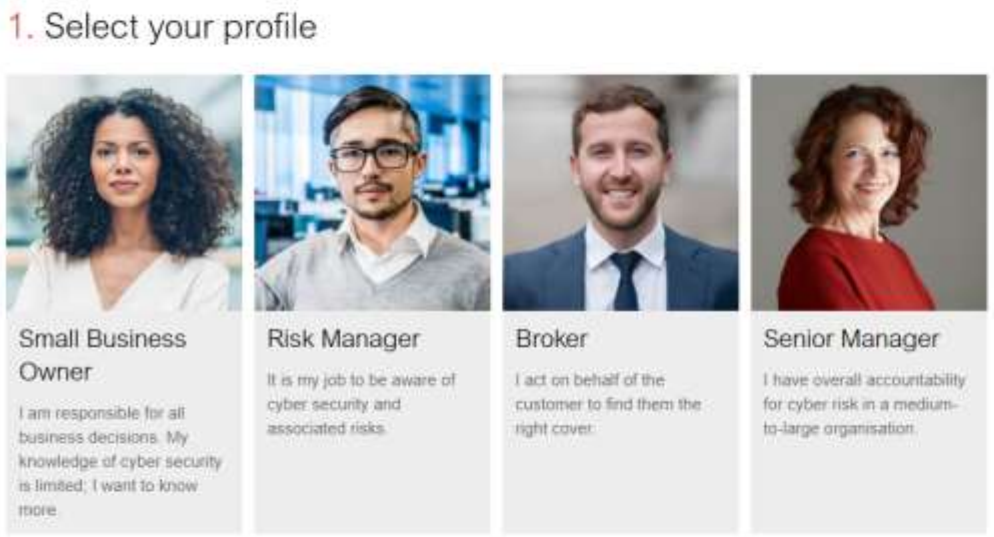
## Post-breach Services (Assistance Coverage): Description, Exclusion and Limits (Families)

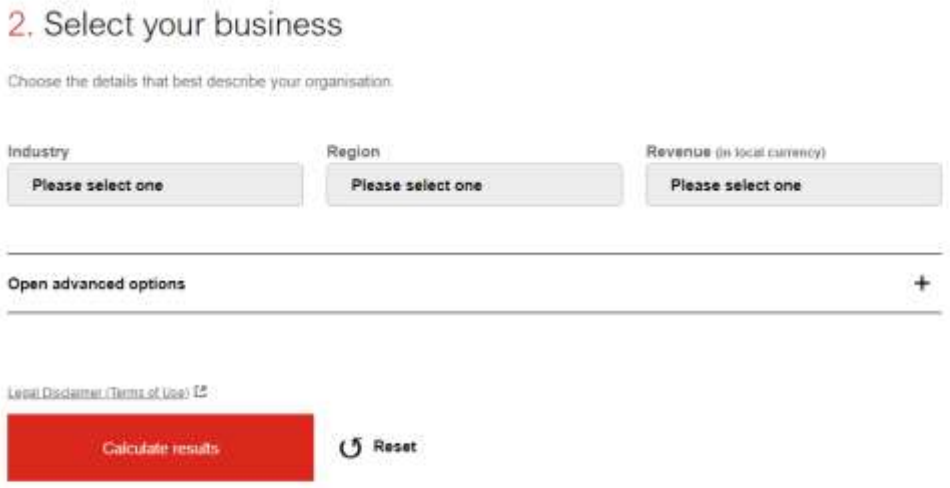
| | Description | Exclusions | Limits | |
|---|---|---|---|---|
| | | | Plan Base | Plan More |
| **Technical assistance** | The Technological Assistance guarantee covers the following services:<br>a) Remote Technical Support<br>The Assistance Service will provide the “Pessoa Segura” by telephone with technical helpdesk support in order to identify and resolve problems reported regarding the operation of the equipment. Whenever necessary and possible, technical support will be provided through remote access.<br>This service is available 24 hours a day, every day of the year.<br>b) Technical Support at Home<br>Whenever the Assistance Service verifies the impossibility of solving the problem via Remote Technical Support and there is no repair laboratory in the vicinity of the Policyholder's Permanent Residence, the latter will send a technician to his residence to solve the problem.<br>c) Pickup & Return<br>Whenever the Assistance Service identifies that it is more appropriate to solve the problem in a laboratory environment, avoiding a prolonged presence in the Insured Person's residence, a transport service will be provided for the equipment in question.<br>d) Laboratory Service<br>Whenever technical support proves to be insufficient, either through remote support or home support, this will be done in laboratory stores. | 1. The provision of in-person services out of hours or with response times of less than 24 hours;<br>2. The provision of face-to-face services in a location other than the policyholder's residence;<br>3. The provision of training services in the use and maintenance of equipment and respective applications;<br>4. The provision of computer assistance services for unlicensed software; | Non-included | Unlimited |

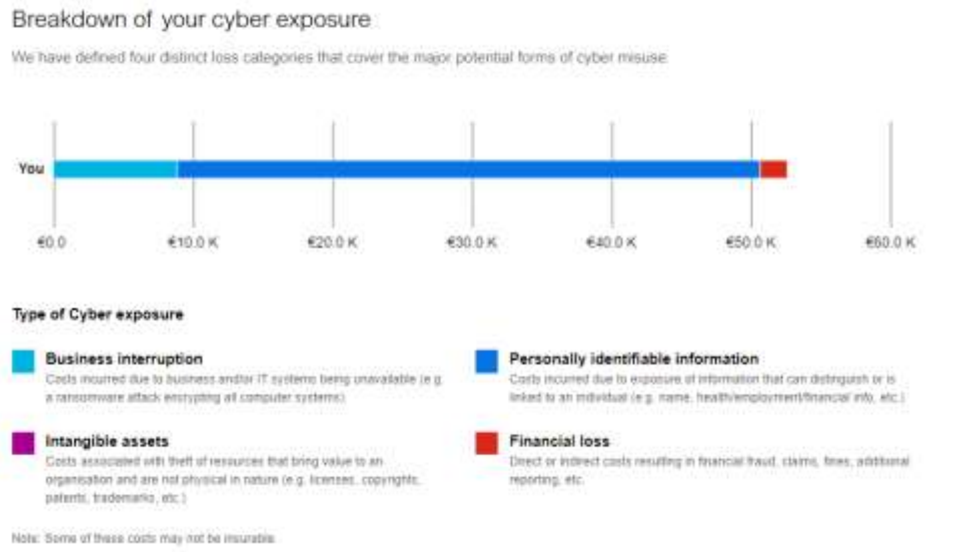
## Agenda

## Risk Assessment Tool - Best Practice (I/II)

| Best Practice | |
|---|---|
| Innovarisk UNDERWRITING | **Cyber calculator:** a tool aimed to help raise awareness about the potential financial impact of a cyber-attack (designed for educational purposes only), allowing companies to:<br>• Get an **exclusive view** of their possible cyber exposure and the value of the data<br>• Get **insight** into the **types of cyber-attacks** that they can face<br>Therefore, businesses can make more informed decisions about how to manage the risk, which can be a combination of risk reduction, risk transfer, and risk retention. |



Back to Presentation

## Risk Assessment Tool - Best Practice (II/II)

### Type of attackers likely to target your organisation

Cyber attackers typically fall into four broad categories:

**Disturbance - 25%**
Attackers motivated by social or political goals rather than money.

**Espionage - 0%**
Highly sophisticated hackers motivated by access to intellectual property or other commercially sensitive data.

**Bulk Crime - 75%**
Financially motivated attackers who tend to attack large and random groups of targets.

**Organised Crime - 0%**
Sophisticated hacking groups who target individuals or groups of organisations with the specific intent of large scale financial crime.

Note: all numbers have been rounded to the nearest whole percent.

### Share your results

Share your results with stakeholders and get started on your journey to making better cyber risk-based decisions. Or view the page and then bookmark it for future reference.

Email your results page

View your results page

### Contact us

To find out more about cyber insurance, cyber risk management or your results, contact us below.

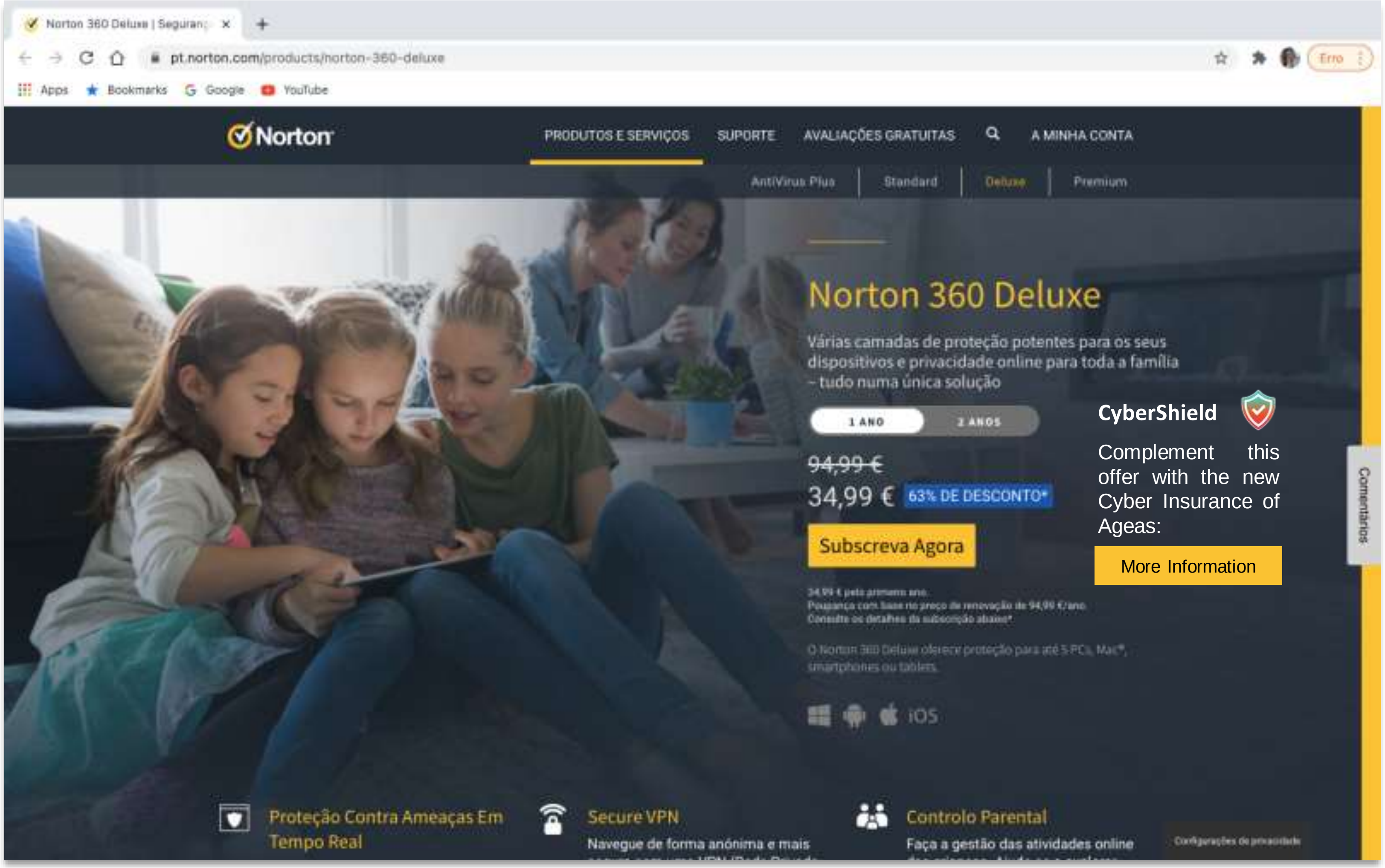
Contact Hiscox

If you would like to find out more about the Cyber Exposure Calculator, please read our frequently asked questions

*Sources*: *Innovarisk*

## Agenda

## Norton's Website




**Objectives of announcing the product in Norton's website:**

**A. Raise Attention**

With the lack of cyber insurance market knowledge from individuals, Ageas can raise attention to its product for people that are already aware of cyber dangers but are not yet considering a cyber insurance product.

**B. Build Trust**

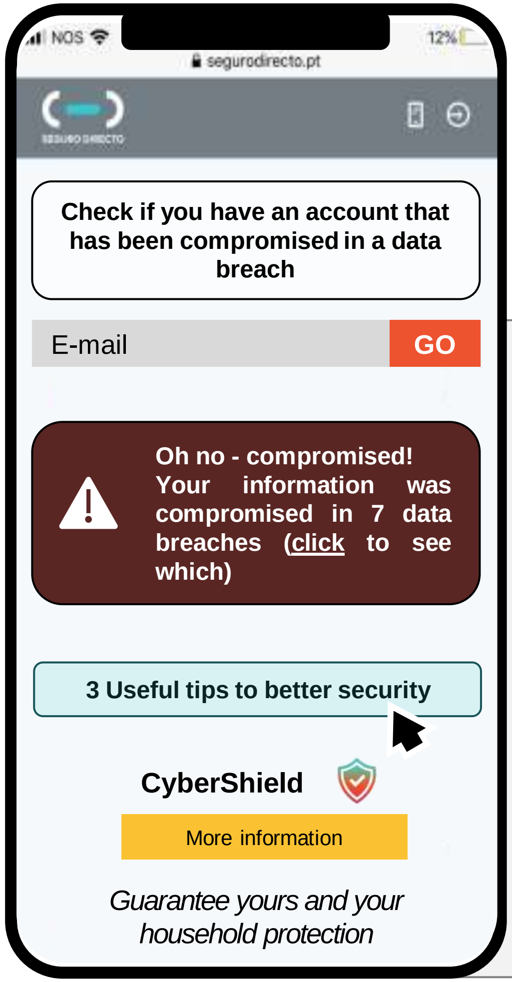
With Norton's already built reputation in the cybersecurity industry, Ageas will be seen as a trusted partner.

Ageas should leverage on its partnership with Norton to promote CyberShield.

Since the recommended packages are Norton 360 Deluxe and Norton 360 Premium, a message with a suggestion to complement the product with Ageas cyber insurance should be displayed next to these packages.

## Risk Assessment Tool

### Objectives of the Risk Assessment Tool:




**A. Raise Awareness**

Individuals can check if they were victims of identity theft, due to a data breach or hacking.

**B. Interactive First Contact**

A positive interaction may lead to a higher conversion rate.

**C. Identify Clusters**

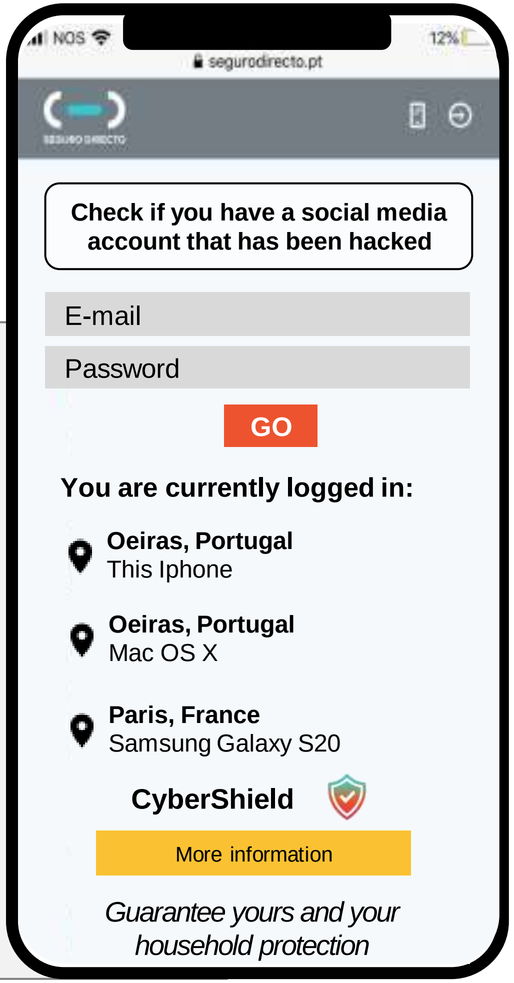
By inputting their key data, individuals will be easily identified and grouped in their clusters.

**Checking for data breaches:** tool displayed on the brands' website

1. The tool inputs the e-mail of the potential client;
2. Outputs the result: if the e-mail has been exposed due to a data breach or not;
3. Gives the option to check in which websites the e-mail was compromised (so that the potential client can take security measures) and three (or more) tips to improve cybersecurity (e.g., use complex passwords and multi-factor authentication);

**Checking for identity theft:** tool displayed on the brands' website

1. The tool inputs the e-mail and the password of the social media account (a direct connection to the app can also be done to avoid this step);
2. Outputs the result: all the locations and devices where the account is logged in;



## Social Media Strategy: Content Examples (I/III)


**ageasseguros** • Follow

**ageasseguros** Joana is already using the new program CyberShield, on her daughters' device.
Check @joana advice on how to protect your family and yourself from the biggest cyber threats. And with the new program CyberShield, get the extra protection and guarantees you need! #Ageas #CyberSeguro #CyberShield

3 d

**raquelbrites** 🙌👏
1d 1 like Reply

**madalenasangalho** 😍🤝
1d 1 like Reply

**afonsogomes** Where should I ✍?
1d 1 like Reply

**1.498 views**

3 DAYS AGO

Add a comment…. Publish

### Example 1: Instagram Post

**Objectives of Social Media Posts:**

**A. Raise Awareness**

To tackle individuals' lack of awareness both to cyber risks and cyber insurance offers, Ageas should share Social Media Posts about the product.

**B. Build Trust**

By sharing positive reviews of CyberShield, potential clients' willingness to buy in the consideration stage of the customer journey may increase, since Ageas will be perceived as a trusted partner.

Ageas should share **testimonials** with the suggested partners on its Social Media and, if possible, on the partners' Social Media pages to reach a larger audience.

**Post description:**

- Simple and direct description of the post (linked to the testimony's page);
- Use of hashtags (to boost the post's views) related to the brand and product.

# APPENDIX 31 – GO-TO-MARKET PLAN (B2C)

## Social Media Strategy: Content Examples (II/III)


### Example 2: Instagram Post

Ageas should also share **the risk assessment tool** on its Social Media and suggested partners' Social Media pages.

**Post description:**

•Simple and direct introduction of the risk assessment tool;

•Use of hashtags (to boost the post's views) related to the brand and product.

•Positive reviews;

•Direct link in the partners' profile to the risk assessment tool on the brand's website.

## Social Media Strategy: Content Examples (III/III)


**Example 3: YouTube Video**

Ageas should leverage on YouTube's large audience and advertise its new product through this channel. By partnering up with renowned technology and, specifically (if possible), cybersecurity content creators, Ageas will reach an audience possibly on the consideration stage of the customer journey. These customers will be positively influenced by the good reviews provided by the partners and, therefore, may be more willing to buy CyberShield.

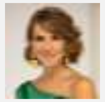
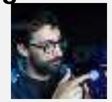
**Video description:**

- Comprehensive description of the product and its features;
- Main benefits;
- Comparison with direct and indirect competitors (PoP and PoD).

# APPENDIX 31 – GO-TO-MARKET PLAN (B2C)

Back to Presentation

## Social Media Strategy: Other Potential Partners

| PARTNERS | SELECTION REASONING | | CHANNEL |
|---|---|---|---|
| **Cláudia Vieira**  | • Family-oriented;<br>• More than 1.1M followers; | • Top 10 influencers in Portugal;<br>• 3.20% engagement rate. | Instagram |
| **Rui Unas**  | • Family-oriented;<br>• More than 801.6K followers; | • Top 20 influencers in Portugal;<br>• 0.70% engagement rate. | |
| **A Pipoca Mais Doce**  | • Family-oriented;<br>• More than 677.9K followers; | • Top 30 influencers in Portugal;<br>• 2.50% engagement rate. | |
| **Ana Guiomar**  | • Reaches customers between 25-35 years old;<br>• More than 544K followers; | • Previous victim of a cyber attack (identity theft). | |
| **Filipe View**  | • Tech-oriented;<br>• More than 3.3M accumulated views; | • More than 47K subscribers. | YouTube |
| **Geek'alm**  | • Tech-oriented;<br>• More than 141K accumulated views; | • More than 2.5K subscribers. | |
| **Hugo Medeiros**  | • Tech-oriented;<br>• More than 1.3M accumulated views; | • More than 11K subscribers. | |

## Agenda

# APPENDIX 32 – UNDERWRITING PROCESS (I/II)

## Language Risks

**Perceptions of cyber insurance in EMEA**

| | Expect to be included |
|---|---|
| Incidents | External attacks by cyber criminals |
| | Malicious or criminal insiders |
| Coverages | Forensic and investigative costs |
| | 3rd party liability |
| | Legal defence costs |
| | Replacement of lost or damaged equipment |
| Services | Access to cyber security forensic experts |
| | Access to legal and regulatory experts |
| | Assistance in remediation of the incident |

| | Don't expect to be included |
|---|---|
| Incidents | Human error, mistakes and negligence |
| | Incidents affecting business partners, vendors or other 3rd parties that have access to your company's information assets |
| | System or business process failures |
| Coverages | Brand damages |
| | Revenue losses |
| | Communications costs to regulators |
| | Regulatory penalties and fines |
| | Notification costs to data breach victims |
| Services | Identity protection for breach victims |
| | Credit monitoring for breach victims |
| | Assistance in the notification of breach victims |
| | Advanced warnings about ongoing threats |
| | Access to specialised technology and tools |

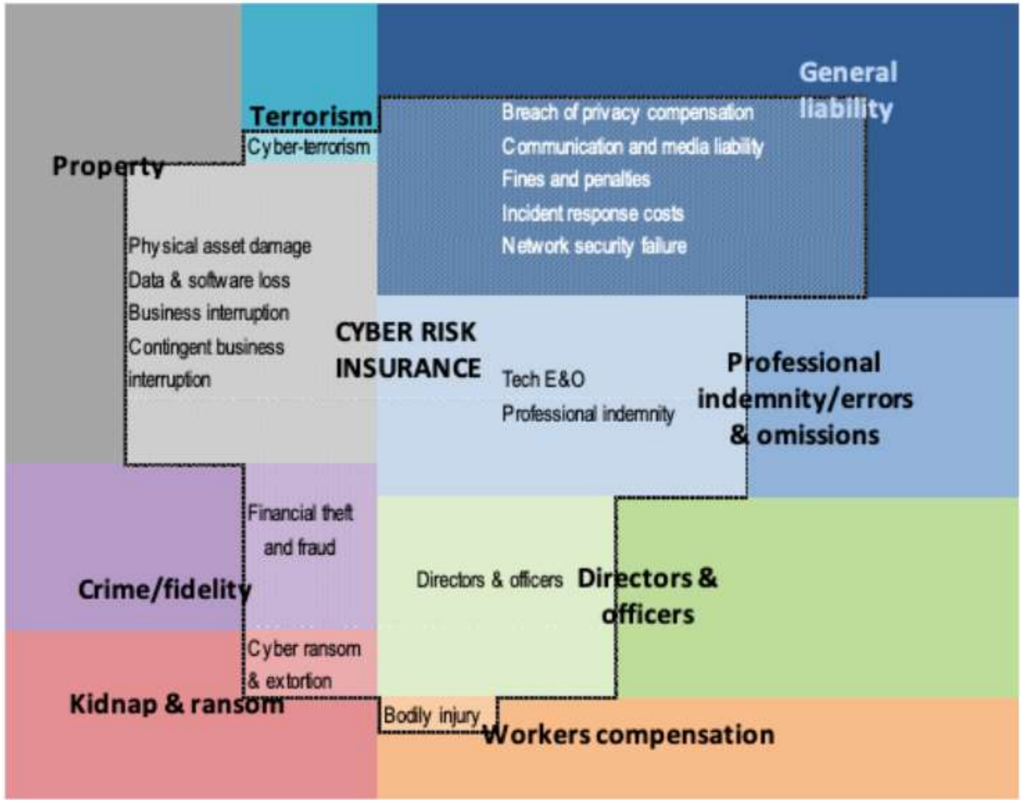
*Respondents considered what incidents, coverages and services are included in cyber insurance*

- *"Expect to be included" is aspects of cyber cover 70% or more agree with*
- *"Don't expect to be included" is aspects of cyber cover 30% or less agree with*

**Sources**: *OECD*

## Silent Cyber Risks

**Schematic illustration of non-cyber insurance policies that can have claims filed due to cyber perils**




*Sources*: OECD

## Solutions for Language Risks (I/IV)

### Information Sharing and Analysis Centres (ISACs)


### Taxonomy Best Practice I (ENISA)

**FIRST PARTY LOSS**
**direct loss incurred by the insured**

- **Network interruption** loss of business income due to cyber incident, Business interruption, damage to intangible assets
- **Network interruption OSP** loss due to outside provider security or system failure
- **Network interruption: System failure** loss due to system failure or human error
- **Cyber Extortion** cost of ransom payment, cyber specialist
- **Electronic Data Incident** loss due to accidental damage of computer system, e.g. flood
- **Cyber theft** financial loss from fraudulent electronic transfer of funds
- **Data restoration**
- **Extra expense**
- **System clean-up costs**
- **Administrative investigation and penalties**

**THIRD PARTY LOSS**
**liability coverage/ losses to others**

- **Data Protection and Cyber Liability** liability claims, fines
- **Media liability**
- **Goodwill coupon** cost of goodwill coupon
- **Wrongful collection of information**
- **Media content infringement/ defamatory content**
- **Violation of notification obligations**

**OTHER BENEFITS**
**costs and services**

- **First Response** Crisis management/ IT experts, Breach-related Legal advice, Forensic investigation costs, Call Center/ Hotline
- **Event Management** Legal/PR, technical forensic, incident notification
- **Criminal Reward Fund**
- **Credit/ identity monitoring**
- **Communication costs** following damage to reputation

***Sources**: ENCS, ENISA*

## Solutions for Language Risks (II/IV)

### Taxonomy Best Practice II (Lloyd's)

| v1.0 Code | Cyber Loss Coverage: Primary Category | Lloyd's Min. Recommend* | 1st party | 3rd party | Description |
|---|---|---|---|---|---|
| 1 | **Breach of privacy event** | Security Breach of Privacy | 1st | | The cost of responding to an event involving the release of information that causes a privacy breach, including notification, compensation, credit-watch services, and other third-party liabilities to affected data subjects, IT forensics, external services, and internal response costs, legal costs. |
| 2 | **Data and software loss** | Replacement of Lost Data and Software | 1st | | The cost of reconstituting data or software that have been deleted or corrupted. |
| 3 | **Network service failure liabilities** | Security Breach of Privacy | | 3rd | Third-party liabilities arising from security events occurring within the organisation's IT network or passing through it in order to attack a third party. |
| 4 | **Business interruption** | Business Interruption | 1st | | Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a result of cyber attacks or other non-malicious IT failures. |
| 5 | **Contingent business interruption** | Business Interruption | | 3rd | Business interruption resulting from the IT failure of a third party, such as a supplier, critical vendor, utility, or external IT services provider. |
| 6 | **Incident response costs** | Security Breach of Privacy | 1st | | Direct costs incurred to investigate and close the incident to minimise post-incident losses. Applies to all the other categories/events. |
| 7 | **Regulatory and defence coverage** | Regulatory Fines | 1st | | Covers the legal, technical, or forensic services necessary to assist the policyholder in responding to governmental inquiries relating to a cyber attack, and provides coverage for fines, penalties, defence costs, investigations, or other regulatory actions where in violation of privacy law, and other costs of compliance with regulators and industry associations. Insurance recoveries are provided where it is permissible to do so. |
| 8 | **Liability —Product and operations** | Liability | | 3rd | Third-party liabilities arising in relation to product liability and defective operations. |
| 9 | **Liability — Technology errors & omissions** | Tech E&O / Programming ENO | | 3rd | Coverage for third-party claims relating to failure to provide adequate technical service or technical products, including legal costs and expenses of allegations resulting from a cyber attack or IT failure. |
| 10 | **Liability — Professional services errors & omissions** | Liability | | 3rd | Coverage for third-party claims relating to failure to provide adequate professional services or products (excluding technical services and products), including legal costs and expenses of allegations resulting from a cyber attack or IT failure. |

* Cyber insurance coverage categories recommended for capture in Lloyd's initiative for a common structure for cyber exposure reporting data.

***Sources***: *ENISA*

## Solutions for Language Risks (III/IV)

### Taxonomy Best Practice II (Lloyd's)

| v1.0 Code | Cyber Loss Coverage: Primary Category | Lloyd's Min. Recommend* | 1st party | 3rd party | Description |
|---|---|---|---|---|---|
| 11 | **Liability — Directors & officers** | Liability | 1st | | Costs of compensation claims made against the individual officers of the business, including for breach of trust or breach of duty resulting from cyber-related incidents and can result from alleged misconduct or failure to act in the best interests of the company, its employees, and its shareholders. |
| 12 | **Multi-media liabilities (defamation and disparagement)** | Liability | 1st | 3rd | Cost for investigation, defence cost, and civil damages arising from defamation, libel, slander, copyright/trademark infringement, negligence in publication of any content in electronic or print media, as well as infringement of the intellectual property of a third party. |
| 13 | **Financial theft & fraud** | Extortion | 1st | | The direct financial loss suffered by an organisation arising from the use of computers to commit fraud or theft of money, securities, or other property. |
| 14 | **Reputational damage** | Reputational Damage / Public Relations | 1st | | Loss of revenues arising from an increase in customer churn or reduced transaction volumes, which can be directly attributed to the publication of a defined security breach event. |
| 15 | **Cyber extortion** | Extortion | 1st | | The cost of expert handling for an extortion incident, combined with the amount of the ransom payment. |
| 16 | **Intellectual property (IP) theft** | Replacement of Lost Data and Software | 1st | | Loss of value of an IP asset, expressed in terms of loss of venue as a result of reduced market share. |
| 17 | **Environmental damage** | Physical Damage | 1st | | Cover for costs of clean up, recovery and liabilities associated with a cyber-induced environmental spill or release. |
| 18 | **Physical asset damage** | Physical Damage | 1st | | First-party loss due to the destruction of physical property resulting from cyber attacks. |
| 19 | **Death and bodily injury** | Bodily Injury | | 3rd | Third-party liability for death and bodily injuries resulting from cyber attacks. |

* Cyber insurance coverage categories recommended for capture in Lloyd's initiative for a common structure for cyber exposure reporting data.

***Sources**: ENISA*

## Solutions for Language Risks (IV/IV)

### Taxonomy Best Practice III (Chubb's COPE Framework)

*Figure 1 - The table below summarizes this transformation of COPE to Cyper COPE®:*

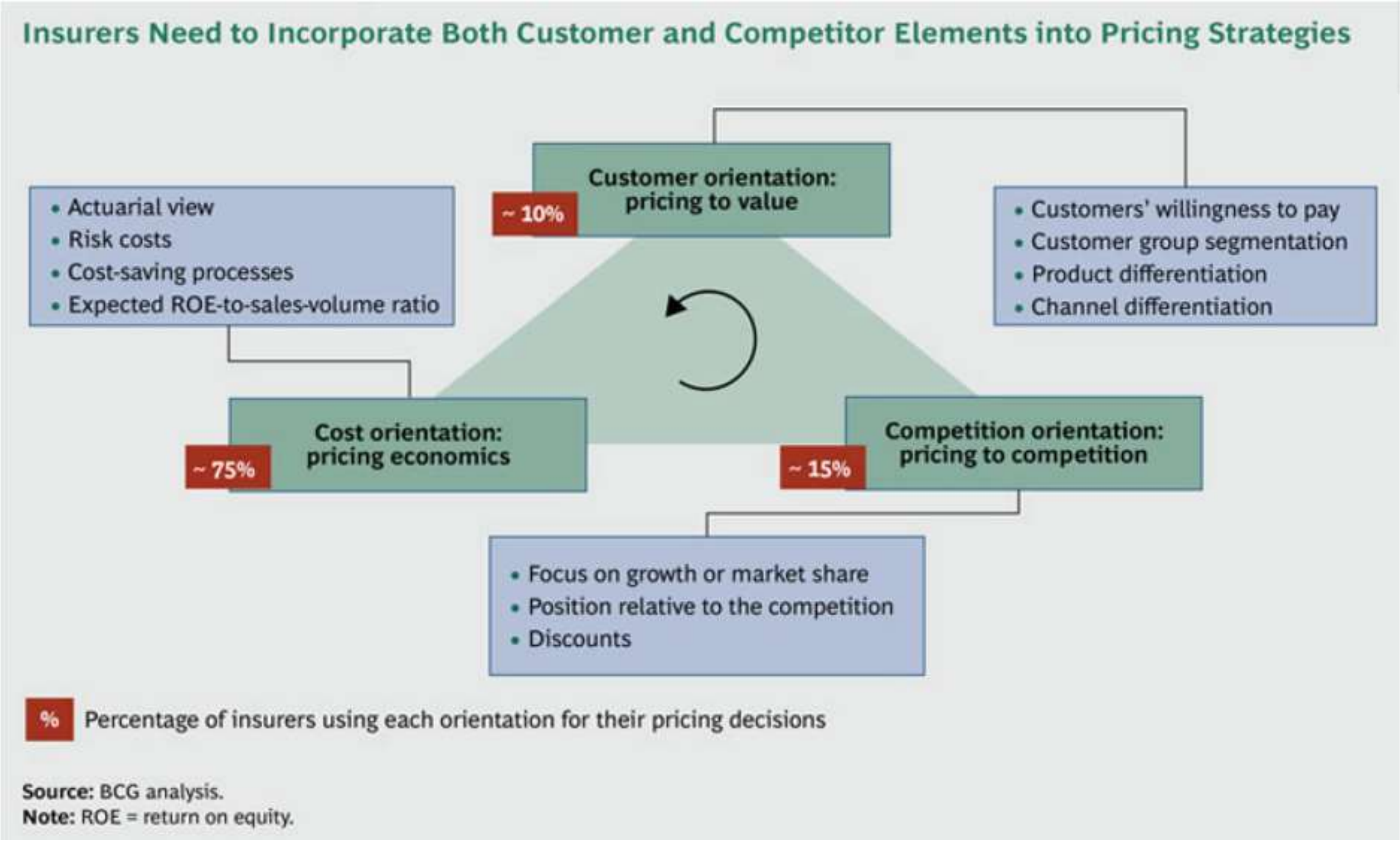
| COPE | Cyber COPE® | Measurement Type | Sample Data Elements |
|---|---|---|---|
| Construction | Components | Objective | Number of endpoints and network connections, software versions, and data center locations |
| Occupancy | Organization | Objective | Policyholder's industry, quality of IT and security related policies, and use of industry standards |
| Protection | Protection | Subjective | Data retention policies, firewalls, monitoring, and incident response/response readiness policies |
| Exposures | Exposures | Subjective | Political or criminal motivation, types of outsourcing, and type/ amount of sensitive information |

**Sources**: *Chubb*

## Agenda

Back to Presentation

## Insurance Pricing – BCG Framework

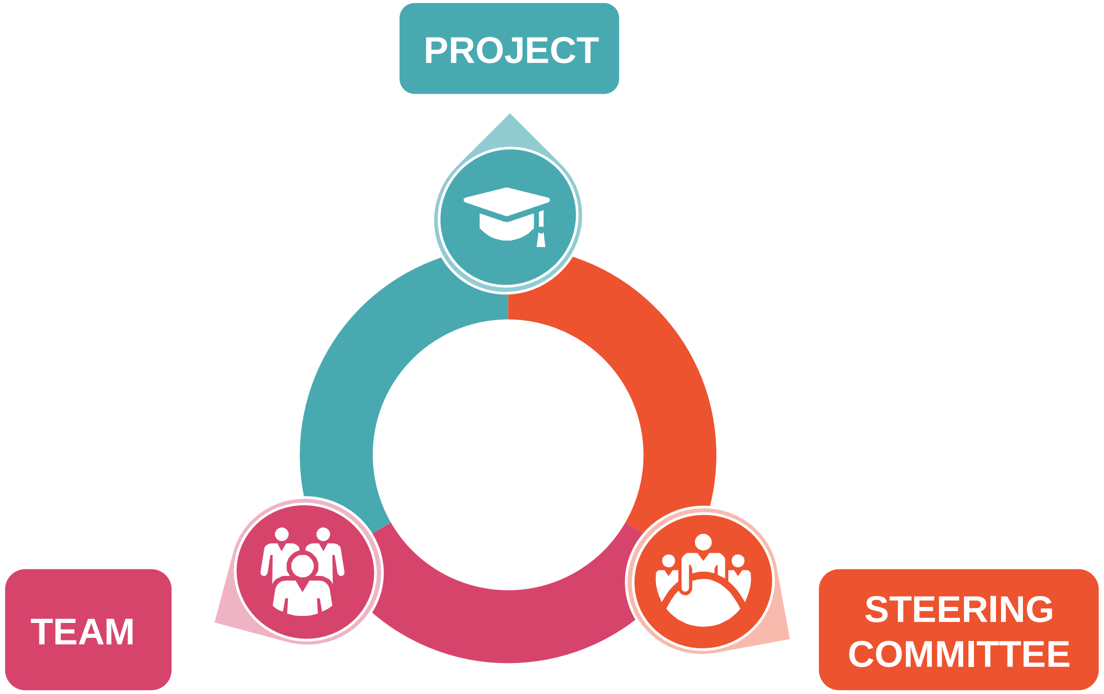



***Sources**: BCG*

## Agenda

# APPENDIX 34 – PROJECT FEEDBACK

- The **relevant theme** (cybersecurity) has increased our **motivation** towards the project;
- Working with the strategy and beyond insurance departments allowed us to **think** “**outside the box**”, which is something we were not expecting in the insurance industry;
- It would have been better to have **more interdisciplinarity** between departments (e.g., technical department) to have a **better outcome** on industry-specific topics.




- Having the **continuous support** of the strategy and beyond insurance team allowed us to **clarify crucial doubts** and **points** throughout the project;
- The **weekly touchpoints** (and later bi-weekly) reflected that our work was relevant and important for the company;
- The **ongoing feedback**, which included both positive and improvement points, made us **grow beyond** our **academic** and **theoretical** knowledge.

- The **availability** shown to schedule the five meetings (from the kick-off to the final meeting) was **fundamental** to make sure we were on the **right track**. Moreover, it made us feel included and **part of the team**;
- The **comments and observations** given during the meetings and later incorporated by us, not only **enabled the alignment of ideas** but also made our **learning curves steeper**.