Jentzsch, Nicola

Research Report

Horizontal and Vertical Analysis of Privacy and Cyber-Security Markets

IPACSO - Innovation Framework for ICT Security Deliverable, No. 4.2 A

Deliverable D4.2 A

Horizontal and Vertical Analysis of

Privacy and Cyber-Security Markets

Project Acronym: IPACSO

Document Author: Dr. Nicola Jentzsch (DIW Berlin)

Project Full Title: Innovation Framework for Privacy and Cyber Security Market Opportunities

Grant agreement number: 609892

Document Control Sheet

Project Number	**609892**	
Project Acronym	**IPACSO**	
Work-package:	**4**	
Last Version:	**January 2015**	
Issue Dates:		**January 2015**
Version 18		

Classification

This report is:

Draft	
Final	X
Confidential	
Restricted	
Public	X

Partners Owning	DIW Berlin	
Author	Dr. Nicola Jentzsch (DIW Berlin, Germany)	Author
Reviewer	Seamus Galvin	Review only (November 2014)
Reviewer	Zeta Dooly	Review only (November 2014)

Acknowledgements

This report benefited greatly from a number of stakeholder interviews conducted in order gain the more applied perspective of privacy and cyber-security markets. The author would like to thank the following persons: Gianluca D'Antonio, Robert E. Beens, Alexander Dörsam, Seamus Galvin, Marcel van Galen, Robert Hayes, Paul de Hert, Gerold Huebner, Aidan Kenny, Alan Mitchell, Nick Wainwright, Toby Weir-Jones, the participants of an internal DIW seminar, and especially Pio Baake.

The output does not reflect the opinion of DIW Berlin.

Table of Contents

List of Abbreviations

CEO	Chief Executive Officer
CTO	Chief Technology Officer
EU	European Union
IAB	International Advisory Board (of IPACSO)
ICT	Information and Communication Technologies
IPACSO	Innovation Framework for Privacy and Cyber Security Market Opportunities
IPR	Intellectual property rights
IT	Information Technologies
NACE	Nomenclature statistique des activités économiques dans la Communauté européenne
NIS	Network and Information Security
PACS	Privacy and Cyber-security

List of Figures

List of Tables

Overview of IPACSO Project

Innovation drives new product realisation and development. Significant opportunities exist for innovation in the privacy and cyber security (PAC) technology space, yet complex market, regulatory, policy, commercial, and economic considerations create several barriers to transforming research outputs into market-centric product and service applications.

In response, Innovation Framework for Privacy and Cyber Security Market Opportunities (IPACSO) will develop a structured knowledge and decision-support innovation framework for identifying, assessing and exploiting market opportunities in the privacy and cyber security technology space. IPACSO will support security innovators, policy makers and research spectrum stakeholders in identifying, assessing and exploiting new ideas and research assets using innovation and market assessment best-practice and guidelines and bringing them to market. Particular emphases will be placed on providing better support for more advanced forms of innovation, particularly radical innovation that has the highest risk but provides the most significant opportunity for disruptive commercial impacts.

IPACSO is an EU-funded Co-Ordination and Support Action (CSA) project aimed at supporting Privacy and Cyber Security innovations in Europe. The key aim is to support ICT Security innovators with State of the Art innovation methodologies and best practices that improve their overall innovation process. IPACSO's main focus is on adapting existing innovation methodologies available in other domains and optimizing these approaches for the PACS market domains. Ultimately, IPACSO aims to combine innovation support modules based on established methods, with new innovation support approaches geared towards the specific needs of the European PACS marketplace where relevant. Market information of high-relevance will also be included in the project, supporting improved awareness amongst target PACS innovators.

Achieving project impact objectives can be challenging for ICT security research projects due to multiple factors and "pain points" described in our reports. We propose that PACS innovators increase the impact of their project results through the adoption & utilisation of the knowledge and methodologies found in the IPACSO innovation framework which addresses the following main goals:

- Assessment of the existing innovation processes used in the PACS domain via in-depth stakeholder engagement.
- Identification of a set of innovation framework requirements, interleaving improved innovation practices and case study scenarios, that support PACS domain concerns.
- Assessment of the existing economic barriers to innovation and identification of the appropriate economic incentives needed to increase security product and service adoption.
- Development of an appropriate knowledgebase and decision support approach that is transferrable to PACS technologies exploiting potential market opportunities.
- Development of effective training, exploitation and dissemination of the resultant IPACSO framework to target stakeholder groups, both during and beyond the project lifecycle.

IPACSO project activities are also aimed to lead towards a structured understanding of concerns considered in the context of wider ICT factors such as Cloud Computing, Big Data, emerging Internets of Services (IoS), Internet of Things (IoT) among other macro trends. In order to fulfil project goals, the work plan is structured in a number of deliverables spread across the following Work Packages:

- **WP1 Project Management:** covers project management and co-ordination activities throughout IPACSO's project duration.
- **WP2 Market Analysis (focus in this document):** delivers a commercial assessment of the PACS domain, identifying the key barriers to effective innovation in bringing PACS technologies to market, supporting innovation framework requirements development and subsequent contributing to the development of the IPACSO framework. This deliverable (D2.2) forms part of this analysis as will be explained in further detail in the following section.
- **WP3 Framework Requirements:** will identify a set of innovation requirements necessary to develop an appropriate and responsive framework for supporting innovation needs around PACS products and services, using analysis of existing state of the art, and stakeholder engagement as a guide. Engagement with IPACSO's Innovation Advisory Board (IAB) members will form a core part of this effort.
- **WP4 Economic Incentives:** will assess current economic incentives and disincentives that influence PACS adoption at present, identifying how such economic factors can be modified to support better PACS innovation, and be reflected accordingly in IPACSO.
- **WP5 Framework Development:** will develop the core knowledgebase and decision-support modules that will form IPACSO, taking relevant findings from WP2, WP3 and WP4 as input.
- **WP6 Training, Exploitation and Dissemination:** will address and implement the training programme used to support adoption and learning around IPACSO, will support outreach and awareness around project activities, and will put a plan in place to support future use of IPACSO outputs.

From an outreach perspective, innovators that work alongside IPACSO will be able to increase their understanding of existing methodologies, best practices, market considerations, economic incentives and share key opinions alongside other peer experts in the PACS domain. Privacy and cyber security innovators who will be reaching out to IPACSO and align with the IPACSO Innovation Framework, will have a valuable set of tools at their disposal designed to help them break barriers to bringing security products to the market and collaborate with other innovators and business support organizations.

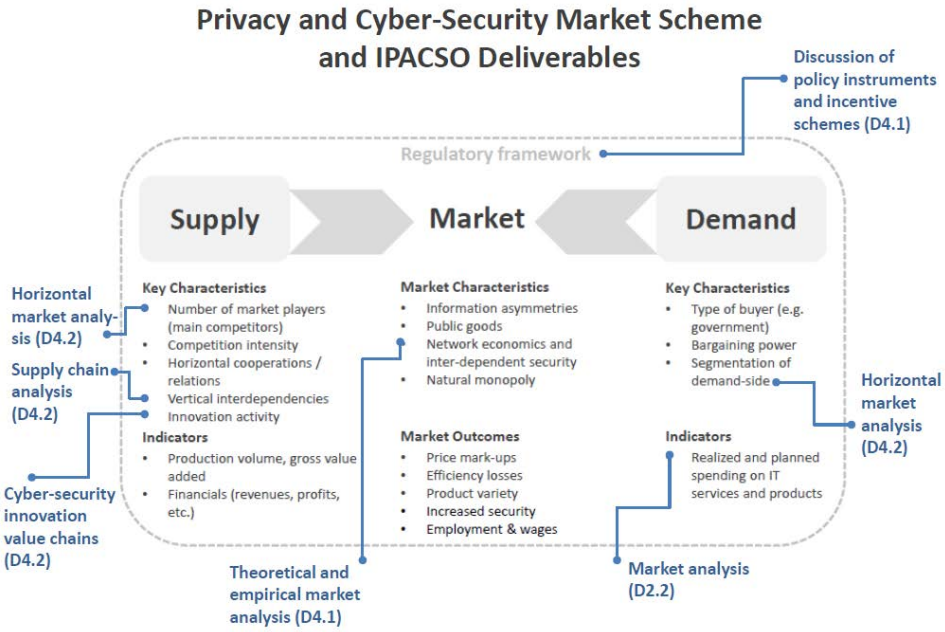
Executive Summary

Deliverable 4.2 (*"Horizontal and Vertical Analysis of Privacy and Cyber-Security Markets"*) provides an in-depth discussion of economic incentives, stakeholder engagement and market opportunities in privacy and cyber-security. This report first introduces the reader to the horizontal market analysis, which covers firms active at the same stage of the production chain in the privacy and cyber-security industry and present key market segmentations.

The report also presents the vertical analysis of players at different stages of the production chain in the PACS industry. These relations are covered as security in the supply chain is of utmost importance: only secure inputs ensure a secure product as final output. The report also covers engagement and assessment of stakeholders in the privacy and security chain and their relation to PACS in the ICT sector. The report gives several case studies on vertical relations and includes an empirical analysis of incentive schemes. The proposed innovation value chain connects inputs and outputs in the production of PACS goods and services and their relation to economic incentives.

Finally, a preliminary scheme on mapping privacy and personal data product and service markets is proposed. Firms active in these markets can be categorized according to their generic value chain, where some use the identification of the user as key input and others do not. The report provides economic incentive templates that enable market players and regulators to potentially better map the markets.

The following scheme outlines in brief the relation of the two deliverables D4.1 and D4.2 to the developed Privacy and Cyber-Security Market Scheme. It enables the reader to see what is covered in the different deliverables and to what deliverable he/she needs to turn in order to find the information of interest.



I. Analysis of Cyber Security Markets

Understanding the market environment, in which firms compete, is a precondition for the understanding of the economic incentives of market players to innovate. This report is intended to facilitate such an understanding.[1] Innovators that gain in-depth knowledge about their relevant market, the players and the regulatory environment, will be able to direct their innovation efforts towards more successful innovations and to stop those early that are not likely to be successful. In-depth knowledge enables identification of market obstacles, production bottlenecks and input dependencies that could become a problem during the production and the rolling-out of new products and services. It will also shed a light on the long-term viability of a business model. Thus, knowing the market environment incentivizes production and innovation and this holds in privacy and cyber-security markets as well as it does in other markets.

At this stage, there is no international agreement on how to define cyber-security or IT security and therefore there is no common standard on how to identify ICT-security or cyber-security markets. The problem is that the inability to identify the cyber-security market impairs the ability to identify trends and forecast important developments in the markets, i.e. how the individual segments develo. It also hampers at the international level the direction of funds into important areas of the cyber-security value chain.

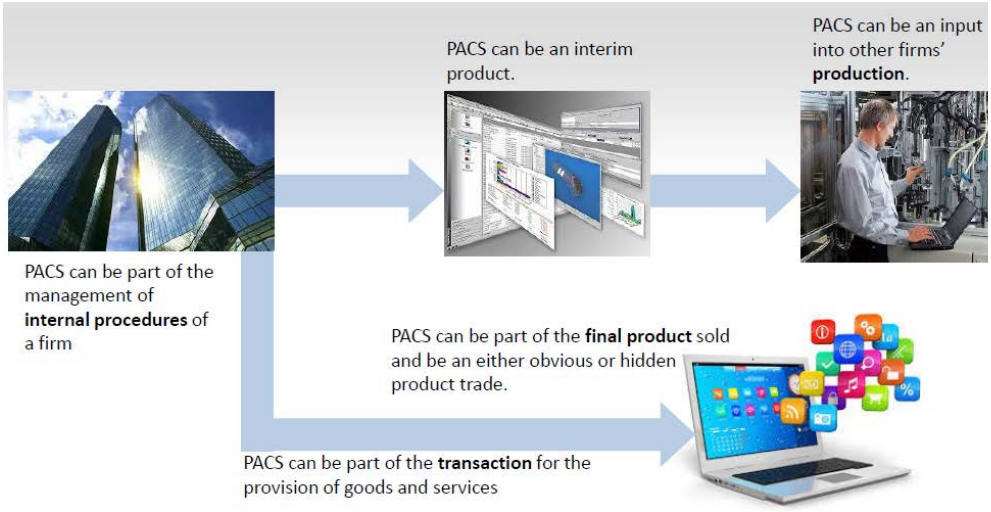
As of 2014, there is no general definition of these specific markets. Various terminologies are used by different stakeholders ranging from IT and ICT security (used by the German government and Eurostat) to cyber-security (UK government and International Telecommunication Union). Other, such as the NIS platform, use Network and Information Security as activity description.

Another difficulty encountered in the market analysis is that cyber-security and privacy are polymorphous product or process qualities: they can be part of internal business continuity procedures of firms, emerge as a quality of a sales transaction or, possibly, result in an interim or final output. The threats and vulnerabilities that emerge in the production and distribution of security and privacy products differ from threats to common goods in their speed, sophistication and potentially large-scale negative impact in relation to critical infrastructure organizations.

Market identification is also difficult, because security and privacy-enhancing features can be embedded as an economic enabler in products and services, which are primarily intended for a use other than securing an asset, e.g. a common Laptop. However, they can also be stand-alone products with the primary goal of securing an asset, such as Anti-virus software or biometric access solutions. Examples of **cyber-security products** include anti-malware software, network intrusion detection, and authentication mechanisms.

[1] This report is a companion report to Deliverable 4.2 (B). Moreover, it is associated with D4.1, which is a state-of-the-art overview of research on cyber security economics and privacy. The present document is an applied perspective on economic incentives as well as horizontal and vertical market analysis.

Figure 1 Privacy and Cyber-security (PACS) in Economic Transactions



Source: The author.

Personal data and privacy products and services have the primary goal of establishing anonymity of natural persons or establishing or maintaining control rights and confidentiality of personal data. Examples include anonymization websites, personal data vaults, and encryption tools[2].. There is not a clear-cut demarcation line between privacy and cyber-security tools and products, as many serve the same purpose. For some products, however, it can observed that their main purpose is information control (such as personal data vaults) and less general cyber-security.

Many qualities of digital products are comparable to other industries, such as the internationalization of the supply chain, the interwoven supplier-buyer relationships, and the vertical integration of large corporations. However, it is observable that increased networking and integration of supply chains can increase vulnerability (e.g. through linkage attack). Therefore, new product developments tackle these vulnerabilities (e.g. out-sourcing of real-time network monitoring). Whether increased integration increases or decreases cyber- and privacy risks must be left to further research.

1.1 Horizontal Market Analysis of Cyber-Security Markets

An initial step is to conduct a horizontal market analysis, i.e. an analysis of the number of players that are rivals at the same stage of the production chain. This also involves analysis of market structure, market segments and the competitive conduct of these rivals. First the market environment needs to be understood in order to further innovation incentives of market players in PACS markets. If the threat of competition is high, the speed of innovation take-over by rivals is high, incentives to innovate will be low. These will be developed into templates presented in the Annex.

[2] Further detail is provided in D2.3 (Section 1.2)

Market Definition and Relevant Players

Market Definition: The cyber-security market is a physical or virtual place, where demand and supply for cyber-security products and services meet.

Relevant Players: In order to identify a player as active in the cyber-security market, the company needs to offer one product line or a portfolio of cyber-security products or services in the market. As discussed below these can span from authentication, authorization and access control to cryptography and system integrity. Players that are active in the ICT market (like Microsoft) are not automatically firms with a separately identifiable portfolio of cyber-security products and services. So while **all cyber-security firms are active in the ICT industry**, by being part of the downstream market, the inverse does not hold. Ideally, the main share of revenue of a player would be associated with the marketing of the cyber-security products.

Some of the players in PACS markets are **end-to-end providers of cyber-security solutions**. End-to-end providers offer solutions that combine software, hardware and services. There are also many specialized firms that are only active in one specific segment, such as IT security consultancy services or encryption providers.

In PACS markets, market analysis is a challenge, because of the diversity of players and the complexity of their relationships and products. It also involves difficult questions about Intellectual Property Rights (IPR), for example, as evidenced by IPR law suits between large IT-corporations.[2]

The stakeholder interviews conducted within the IPACSO-project showed that market players know their competitors very well, but competition varies from segment to segment. For example, while the cybercrime unit of a large IT corporation competes with a consulting firm in the segment of cyber-security consultancy services, the consultancy firm is not a competitor in the segment of software production of the IT company. A rival in the sale of software can be a cooperation partner in another area, such as research and development. Firms in cyber-security markets regularly establish strategic alliances by approving technology exchange, join common products development or marketing efforts.

In digital markets, companies with a wide variety of business models can be direct competitors. Consider, for example, the market for the provision of identity services on the Internet to which an identity card provider may belong as well as a social network or a personal data vault.

To date, there is not a comprehensive literature overview of privacy and cyber-security markets. The **IPACSO WP4 Deliverable – D4.1** refers in section 1.1 to the cyber-security market. The studies quoted therein as well as elsewhere in the IPACSO output (such as in WP2) will be discussed in greater detail below.

1.1.1 CYBER-SECURITY MARKET STUDIES

There is not an extensive literature on horizontal market analysis. Only a few reports are publicly accessible, three selected ones are listed in Table 1 below. Others are expensive industry reports published by consultancies.[3] The author identified four publicly accessible studies, all listed in the aforementioned Table, with the common goal of estimating the size of the cyber-security market in specific countries or Europe. Only three will be discussed for their provision of estimation of a total market size.[4]

Europe: The IDC Emea (2009) study estimates the market size by using indicators such as the IT spending as share of Gross Domestic Product, as well as the IT spending on different categories derived from surveys in the EU. The supply side is covered by using proprietary data, which is claimed to be a representative sample of network and information security vendors. IDC Emea horizontally segments the market in the way most commonly used. Firms can be sorted into the segments of IT security hardware, software and services.

Germany: One recent study is Bundesministerium für Wirtschaft und Technologie (2013), which uses a more narrow IT industry definition (excluding telecommunication) and characterizes the IT security market as an **aftermarket of the ICT industry**. The argument is as follows: the increasing deployment of IT systems increases the demand for security of these systems. The study's authors estimated that in 2012, the German IT security industry produced goods and services of a value of 6.254 million Euro.[5] This is the most transparent study in terms of information used. The authors used a keyword search in the database of a business reporting firm in order to identify the relevant market players in Germany. The same segmentation as above was used: hardware, software and services.

United Kingdom: Finally, the PAC (2013) study on the UK identified over 600 firms that sell cyber-security products. The consultancy states that they used their own database on software and IT services and added for the study hardware and network equipment. Based upon this methodology, they estimate the cyber-security market is worth almost £2.8 billion in 2013 in the UK (roughly 3.5 billion Euro), and that it will grow to over £3.4 billion in 2017 (about 4.3 billion Euro). The authors use several different types of segmentations, for example by buyer organizations (such as government, defence and SMEs & consumers) as well as hardware, software and services.

A standardized segmentation of the cyber-security market would enable European policy-makers to assess the maturity of the different markets, where a dominance of the service-segment indicates greater market maturity. Moreover, it could better be assessed, where the potential security risks lurk, for example, potentially in the widespread use of hardware and software produced outside of the EU. This will be discussed in the section on vertical relations.

[3] Examples are the reports of ASDReports, Gartner, and Marketsandmarkets. The author could not assess the quality and information base of these studies.

[4] Estimations of the market size are not the primary focus of IPACSO. Therefore, the studies are discussed only briefly. Moreover, market sizing differs with the definition of the market.

[5] This number refers to 9.200 companies in Germany including entrepreneurs and self-employed (*Einzelunternehmer und Selbstständige*).

Table 1 Cyber-security Market Analyses

Source	Year Pub	Market	Time period	Segmentation
Bundesministerium für Wirtschaft und Technologie	2013	GER	2005-2012	Hardware, software, services
PAC – Pierre Audoin Consultants	2013	UK	2010-2017	Government (defence & Intelligence, D&I), government other than D&I, enterprises; SMEs & consumers
IDC EMEA	2009	EU-15	2006-2007	Hardware, software, services

1.1.2 CYBER-SECURITY MARKET SEGMENTATION APPROACHES

Market segmentation is a type of analysis used in marketing, which divides a market into segments that group products, consumers and distribution areas based upon common criteria. The approach employed depends on the goal to be achieved.

Some examples of **segmentations** are:

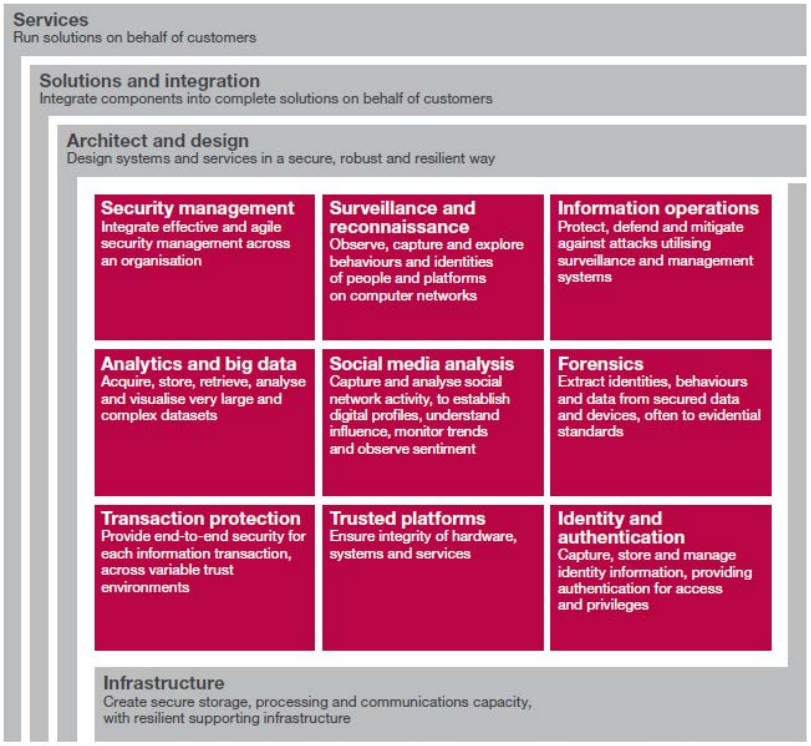
- **Generic type of product/service:** Hardware, software, services (PAC 2013, Bundesministerium für Wirtschaft und Technologie 2013, INTECO 2009 and IDC Emea 2009);
- **Buyer organization:** Government (defence and intelligence, D&I), government (other than D&I), large enterprises (>250 employees), SMEs & consumers (PAC 2013);
- **Security solution:** Infrastructure, systems, contents and governance (PAC 2013);
- **Basic technology:** Authentication, authorization and access control, system integrity, cryptology, etc. (NIS Platform Working Group 3 2014); and
- **By geographical market:** North America, Latin America, Eastern Europe, Western Europe, Africa and Middle East and Asia Pacific.

The sources of these segmentations are referenced at the end of this chapter. Segmentations help to better understand, whether there are clusters of specific consumers that can be provided with similar versions of the product.

Yet another type of segmentation is used by UK Trade & Investment (2012), which combines the horizontal segments with technology solutions (see Figure 2). Consultants are also advising to cluster customers according to the same security or privacy problems they have.[6] Players in different markets (health and banking, for example), could encounter the same security problems and therefore a solution can be sold to both segments. The methodology should be chosen based upon its most valuable differentiation power, i.e., if start-ups find it useful to segment the market along industries (sometimes called 'verticals'), in order to better tailor the product to the specific industry, this segmentation might be most useful.

[6] The author thanks Aidan Kenny for this valuable remark.

Figure 2 Cyber Security Supplier Segmentation



Source: UK Trade & Investment (2012).

The segmentation along product lines (hardware, software and services) might be most useful for policy makers. The reason is that this segmentation allows the analysis of markets (for privacy and cyber-security) along the NACE classification systems. This in turn allows an international comparison of the markets across Europe.

While most stakeholders in the interviews stated that it was clear to them who their competitors were in specific product lines, it is less clear to many start-ups that a company, which is active in segments such as software and services may bundle those offers and provide a far more attractive value proposition as start-up, which is a niche player. Also forward integration threats are often nor clear as well as the risks that exist in vertical value chains. This is discussed in the upcoming sections. A clearer picture on the aforementioned points might make market entry with a new product unattractive.

1.2 Vertical Relations in Cyber-Security Markets

A supply chain connects inputs to outputs by representing different stages of production. Supply chain analysis offers insights into the production of cyber-security and privacy-enhancing goods and services. It allows the description of vertical relationships that exist between market players and their integration at different levels of the production process. Interrelations in the production of

cyber-security products and services are becoming more important the more functions are outsourced to partner firms.

Note that in today's digital markets, it is not sufficient to speak about vertical relationships, as is done here for exposition reasons, networks of suppliers and buyers characterize these markets. Through increased integration, cyber-security risks are shared between ever more partners in the supply network.

The supply chain analysis facilitates also a better understanding of the incentive structures inherent in vertical relations, because the firms' contracts state rules on:

- The **allocation of value added** (and revenues extracted) in the production process between the different actors in the supply chain; and
- The **allocation of risks and liabilities** related to the production and provision of the security goods and services.

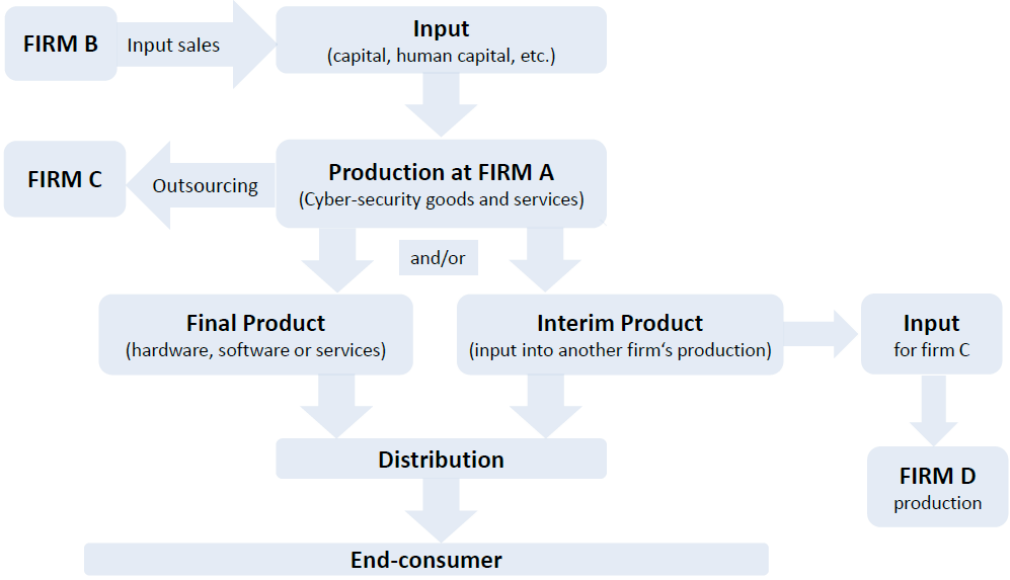
Firms may vertically integrate in order to internalize mark-ups or to offer a broader product portfolio. At this stage, there are a number of open questions. For example, it is an open question whether in cyber-security markets, firms also vertically integrate hardware, software and services in order to obtain full control over the security of their supply chain. It is also not clear, if greater disintegration increases cyber-risks (i.e. through linkage attacks) and therefore negatively affects the resilience of ICT systems.[7]

1.2.1 Deep Integration of Different Supply Chains

While many still see the supply chain as a physical entity, digital services and product provision allows companies to **deeply integrate into each other's supply chains**. One example is the outsourcing of real-time surveillance of networks to IT-companies. Another are e-forensics and e-discovery, where the contracted consultant scans vast amounts of diverse internal and sensitive documents (PDFs, e-mails, Word documents) and therefore obtains deep insights into a firm's business dealings and secrecies. As stated above, in order to deliver secure cyber-security products and services, the supply chain needs to be secure. Some interview partners put forth that in Europe there is an over-reliance on products developed outside of Europe.

[7] An example of a linkage attack is the recent Target Stores incidence in the U.S. (The interested reader is referred to Vijayan, J. (2014). Target Attack shows danger of remotely accessible HVAC Systems, http://www.computerworld.com/article/2487452/*cybercrime*-hacking/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html)

Figure 3 Cyber-Security Supply Chain



Source: The author.

Typically, IT companies that offer cyber-security products and services, use inputs such as human capital and technology in order to produce their products. Most companies purchase these inputs from third-parties. Examples are software suites and hardware. Parts of the production may be outsourced, such as network operations. Currently little is publicly known on how the larger European players in cyber-security market are integrated with suppliers and end-users. The analysis of supply chains in cyber-security markets will also show how players are interconnected through **cooperation and licensing relationships**. For example, a company may license another company's technology and embed it into its own product offer. Moreover, in digital markets, cyber-security being no exception, intellectual property rights are important, constituting additional relationships.

The competitive environment can incentivize firms to vertically integrate, if competition is imperfect and causes multiple mark-ups, which then can be internalized in order to set a more competitive price in the final market. On the other hand, out-sourcing can lead to significant cost savings.[8] Outsourcing, however, may also lead to significant security and privacy issues related to the information assets stored in the cloud, for example. In order to provide more applied examples, four case studies are provided, two of large IT-corporations that offer cyber-security products and two of niche players in the segment of services. Case studies on personal data markets and privacy products are provided in section IV.

[8] Examples are cloud-as-a-service or software-as-a-service offers.

1.2.2 Supply Chain Management and the Secure Development of Security Products

The management of secure supply chains is a critical question not only for firms active in the cyber-security business, but also for critical infrastructure industries. In the former, however, industry stakeholders often describe cyber-security as part of their company's DNA: In order to **develop secure products**, product development and production must be based upon **secure processes and inputs**.[9] **And the same must holds for the idea development stage.** Some companies therefore establish an extra monitoring department that ensures whether security products have been developed securely. In the ICT business and the ICT security business, secure supply chain management includes software, hardware, business procedures and overall system architecture. Vulnerable software aside, hardware is also exploitable (e.g. by containing manipulated microchips). Further, hardware and software interact and both depends on each other.

The management of cyber-secure supply chains is also important in critical infrastructure organizations including banking and finance, water and utilities, and the health sector. These are – as end-users of products and services – at the final stage of the chain that needs to be secure in order to allow a secure operation of critical infrastructure.

Since no stakeholder claims that there is a 100% security, we must speak of the best level reachable given existing knowledge and technology and given the best effort invested.

Due to the complexity of cyber-security products, only a generic model of vertical relations in digital markets can be provided here in order to point to the aforementioned security issues.

1.2.3 Case Study of Large IT-Enterprises in Cyber-Security Markets

HP: HP is a technology company headquartered in the U.S. In general, the company integrates cyber-security features in its products, but also markets a portfolio of extra cyber-security products, services and research.[10] HP analyses security needs of customers such as large enterprises and governments, and provides products fitting into their respective security frameworks. It also provides security software and solutions that integrate information correlation, application analysis and network-level defence.[11] Depending on the market segment, competitors include firms such as Detica, IBM and consultancies such as Accenture. Cooperation and supply-relations occur in a number of ways, such as licensing of technologies or partnering with firms for the provision of integrated products.

SAP: A rather new player on the cyber-security market is SAP. The company is a software producer based in Germany, which also offers analytics and Big Data services, as well as supply chain and customer relationship management solutions. The main customers of SAP are large enterprises. As of 2014, SAP also starts to provide threat detection solutions to these clients.[12] In addition, SAP has

[9] The same holds for services.

[10] See the company's specific website: http://www8.hp.com/us/en/business-solutions/security-overview.html.

[11] This is quoted from the aforementioned website.

[12] See also the company's website: http://scn.sap.com/community/security/blog/2014/09/02/upcoming-ramp-up-for-sap-enterprise-threat-detection and http://www.sap.com/services-support/svc.html

consultancy services for the implementation of new products. Depending on the market segment and product line, SAP has different competitors, among them Intel, for example.

1.2.4 Case Study of Niche Players in Cyber-Security Markets

ESPION: Espion is an IT consultancy business based in Ireland, specializing in information security testing and compliance auditing as well as in digital forensics and e-discovery. Security has been described as a core strategic ingredient into Espion's consultancy business, including secure technical and rights infrastructure and personnel that are trained on awareness. Key competitors in this business are global IT consultancies such as Deloitte, PWC, Ernst & Young as well as Accenture. The company uses bespoke software tools to support several key in-house procedures around service delivery, as well as leveraging several software platforms from third parties.

ANTAGO: Antago is a small consultancy company based in Germany that provides security scans to customers. The company differentiates itself from providers of penetration testing by mostly using software that is developed in-house in order to fully understand the operations conducted. The main customers of the company are energy companies, telecom and IT companies as well as Internet providers or Utilities. In Germany, there are a number of competitors, such as Syss GmbH and LSE among others, most of these being SMEs.

II. Cyber-security Innovation Value Chains

The speed of innovation, short product cycles and complexity of industrial relations ranging from competition to coopetition[13] are signature aspects of digital markets. Moreover, in ICT industries innovation is of special importance, because of the dynamics of technological advancement. This advancement alters continuously the threat and vulnerabilities landscape created by ICT deployment.

Generic models of innovations are provided in Deliverable D3.1 of the project.

Innovation is a strategic decision of companies in competitive markets. However, the majority of observable innovation in cyber-security and privacy markets is best described as incremental. This means that much of the innovation is a product or service improvement, but not a radically new development that forces businesses to re-organization or leads to the emergence of wholly new markets. As became clear from the stakeholder interviews, disruptive innovations in cyber-security and privacy will largely depend upon deployment of disruptive ICT-technologies, following the logic that cyber-security is an aftermarket of the ICT industry.

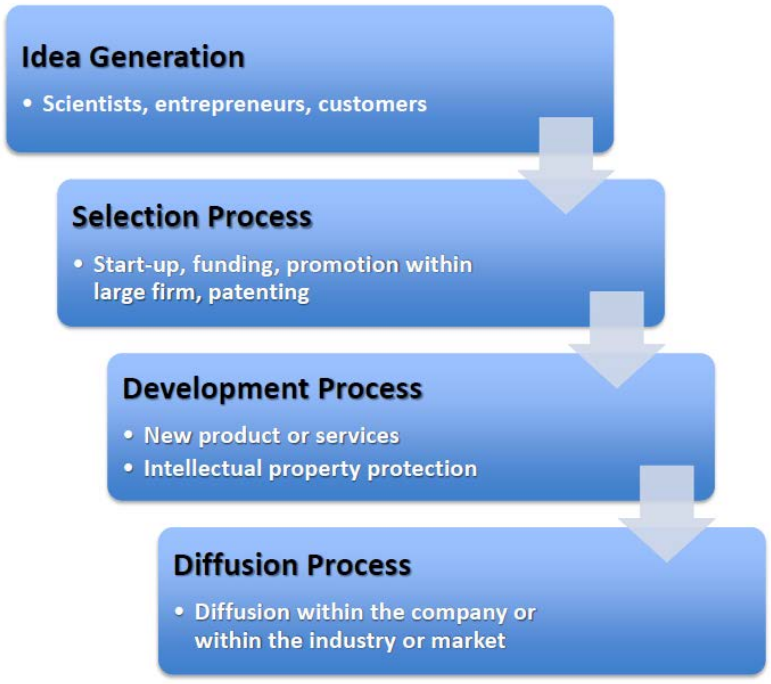
Product or service innovation processes can be also characterized as stages of a value chain. Such an innovation value chain is a **product-centric view that connects inputs into product/service innovation with innovative products/services as outputs.** "The innovation value chain view presents

[13] In the context of this report, the term describes situations, where competitors cooperate.

innovation as a sequential … phase process that involves idea generation, idea development, and the diffusion of developed concepts."[14] This type of model is presented in Figure 4.

The steps involve idea generation, the idea selection process, development and diffusion processes.

Figure 4 Innovation Value Chain

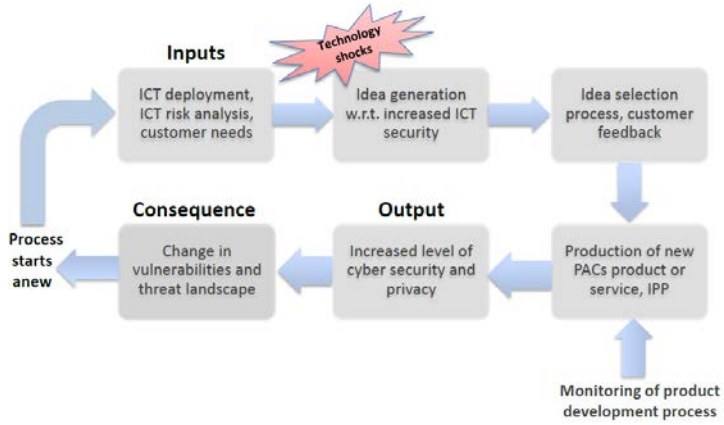


Source: Ljepava (2011) with modifications by the author.

In order to obtain a model that reflects innovation in the cyber-security and privacy markets, the innovation value chain above can be linked with particulars of development processes in cyber-security and privacy markets and the digital supply chain model presented above. Due to the complexities of the industrial relations and the products produced, only a generic model of a PACS innovation chain can be represented here.

[14] Hansen, M.T. and J. Birkinshaw (2007).

Figure 5 Privacy and Cyber Security Innovation Value Chain



Source: The author.

The key inputs for the production of privacy and cyber-security innovations are the employment of ICTs, risk analysis and in many cases, conversations with customers in order to assess their security needs. Ideas may be then generated by individuals, groups or in networks within firms. For most firms, the 'innovation procedure' is simply called product development. The idea selection phase involves discussions within the company, but also with customers. Finally, once an idea has passed the selection stage and enters the production stage, Intellectual Property rights have to be secured and specific technical standards have to be observed.[15]

A **particularity of the innovation cycle in the privacy or cyber-security domain** is the fact that in order to establish a cyber-secure product or service, end-to-end security must be implemented already in the innovation phase.[16] It is clear that there is no possibility to achieve 100% security. **However, the goal of most stakeholders is to achieve the best result given available knowledge and limited resources. Moreover, one stakeholder noted that the goal was to raise the bar until the costs of decrypting a message, for example, by far surpasses the benefits.**

The Software Assurance Forum for Excellence in Code (SAFECode), an industry-led, non-profit organization based in the U.S., promotes best practices for developing more secure and reliable software, hardware and services.[17] Moreover, there are now draft standards such as ISO/IEC 27034 (Information technology — Security techniques — Application security) that provide "guidance on information security to those specifying, designing and programming or procuring, implementing and using application systems, in other words business and IT managers, developers and auditors, and ultimately the end-users of ICT."[18]

[15] A product may also have to adhere to certain regulatory requirements, e.g. specific data protection standards. The product requirements are not discussed in greater detail herein.

[16] See also the discussion on NIST standards in section 4.3.

[17] Quoted from the association's website: http://www.safecode.org/about-safecode/

[18] Quoted from the website: http://www.iso27001security.com/html/27034.html

For firms active in these markets, innovation cycles will look different for individual product or service segments. This became rather clear when the interviewees were asked about their innovation procedures.

Finally, the deployment of the innovation ought to lead to increased levels of cyber-security, which in turn change the vulnerability and threat landscape in ICT deployment, not only at company level, but also through integration in other firm's supply chains.

All in all, the horizontal market analysis sheds light on growth segments of the market, whereas the vertical analysis and innovation value chain sheds light on security risks and points of contention in vertical relations.

III. Economic Incentive Schemes

The stakeholder interviews identified a number of issues concerning the incentivization of cyber-security and privacy, some validating the points already discussed in the **IPACSO WP4 Deliverable – D4.1** with their costs and benefits.

The stakeholder interviews showed that most of them understood the incentive-based notion around privacy and cyber-security very well. Moreover, most could clearly argue what schemes would be preferable in terms of adoption and what schemes are seen as less effective. It must be stated that the stakeholders only represented industry views.

The industry-level and firm-level incentive schemes that were discussed with stakeholders cannot be quantified in their costs and benefits due to a lack of data. For example, it cannot be estimated what costs and benefits would be associated with the adoption of tax reductions as this in itself would constitute a research project. Moreover, most stakeholders were not in a position to give estimates on costs and benefits, but felt confident to give a general assessment of effectiveness of some of the measures presented in Table 2.

As included in **IPACSO WP4 Deliverable – D5.1** there are also a number of questions regarding the operating environment. In order to have a complete set of incentive schemes, the content included in the aforementioned Deliverable is translated here into the matrix version (see **ANNEX 3**).

Table 2 Incentive Schemes and their Effectiveness: General Assessment

Incentivization	Measure	General Assessment
Industry-level		
Public procurement and buyer power	The public sector typically chooses the cheapest provider of service, where cyber-security does not play a role, respective legislation should change to more actively demand secure products and service	This was seen as a very effective tool to improve on cyber-security offers in the market
Public procurement and privacy requirements	EU should set as funding requirement the explicit consideration of the personal data and data protection implications within any Big Data, Internet of Things, Open Data or other project. They should not get funding if they ignore this issue.	This was seen as a very effective tool to improve on privacy offers in the market
Tax reductions	In order to incentivize investments in cyber-security products and services, adequate tax reductions for such investments ought to be implemented	This was seen as a very effective tool by industry stakeholders to incentivize investments in cyber-security
Whistleblowing Platform	A secure whistleblowing platform could facilitate the discovery of security breaches and data leaks. Moreover, it could increase the risk of disclosure to firms and incentivize investments in security	This was not seen as a very effective tool for the reason that most industry players already should be aware of the risks and should not be surprised by data scandals
Standards		
Liability changes	For companies that can demonstrate that they have been diligent* in their risk management, there ought to be a reduction in the liability for security breaches	While this was seen as an effective tool by some, others stated that it was very important to place liability on the party that knows best what is was doing in cyber-security
Firm-level		
Access to advanced training	If a company invested in cyber-security technologies and procedures, it ought to obtain priority for advanced training	This scheme was seen as important, but not as important as tax reductions or liability clarification
Funding of innovation and development activites	EU should shift focus of innovation funds from privacy and privacy- enhancing technologies to personal data empowerment	This type of funding was seen as an important tool to further developments and innovation in personal data markets
Reward and strengthen activities such as cyber-exercises	In order to obtain a change in behaviour of firms, (international) cyber-exercises should be expanded and access also by SMEs firms enabled	Just as access to training, this scheme was seen as important, but not as important as tax reductions or liability clarification
Adoption of IPACSO tools	Enable IT-personnel by providing tools to convince their CEOs on need to invest more into a company's cyber-security governance and technologies.	Especially the provision of work tools for CTOs such as standard justification letters (summarizing why there must be more investment in ICT) was seen as helpful to improve on Cyber-security investments

Notes: *According to one stakeholder, proof of diligence is satisfied, if a company has invested in cyber-security, senior management is directly involved in cyber-security matter, the company underwent annual security audits and in case of a security incident, notified the authorities and the affected parties. Source: IPACSO stakeholder interviews.

In fact, policy makers need to tackle the improvement of incentive schemes at several levels, the industry and the firm level.

3.1.1 INNOVATION PROCESSES AT FIRMS

The stakeholders explained in the interviews, that their innovation procedure is the product development process in the company. The larger IT corporations have research or developer groups that discuss ideas. While, for example, in Germany there is an Employee Invention Right (Arbeitnehmererfindungsrecht), one stakeholder explained that his company incentivizes good ideas with additional monetary rewards in order to establish an innovation culture. Several stakeholders stressed that it is important to give employees the freedom and time to innovate.

Some ideas also arise in conversations with the customers or are in turn shared with customers. Typically, if they find the idea worthwhile, it is pursued further. Some innovations are even ideas of customers. However, one stakeholder cautioned that involving the customer intensively in the innovation process can raise expectations that the company then needs to fulfill.

3.1.2 TYPES OF INNOVATION

The interview partners stressed that innovations in cyber-security can also take **different forms.** While much of the innovation is **incremental product improvement** (e.g. in encryption), some are major changes based upon advances in technology or data availability (such as real-time threat detection through Big Data analysis).

Moreover some general ICT innovations are a simple **repackaging of components** that change the industry quite a lot. One example mentioned in this respect was the IPod.

Other cyber-security innovations are, in fact, taking **a step back (artificial degradation)** by dramatically slowing down the speed of information processing as done in throttling: "If virus-like activity occurs, Virus Throttle will slow down the propagation and notify the IT administrator."[19] This technique significantly slows and reduces computer infections in networks.

However, the most difficult to achieve is **disruptive innovation**. Disruptive innovation would not only lead to the development of new markets, but also render business reorganization necessary. According to one stakeholder, disruptive innovation occurs only in cyber-security and privacy products as well as services once disruptive technology changes have occurred.

[19] HP Technology Brief (2005). HP Virus Throttle technology: Stealth Defense against malicious code in Microsoft Windows environments, http://h10032.www1.hp.com/ctg/Manual/c00369532.pdf.

IV. Markets for Personal Data Products and Services

In the past 30 years advances in ICT deployment have led to a large-scale increase in the collection and processing of personal data.[20] This has led to thriving markets for products that consist of or are based upon personal data and its analysis. Examples include direct marketing and credit reporting, where millions of consumer profiles are sold on a daily basis as well as user profiles compiled from different Internet sources. Data protection laws limit the possibilities for product and service development in this market.

In **IPACSO WP4 Deliverable – D4.1** the economic concept of personal information is discussed as well as the monetization of privacy and the techniques for the economic valuation of privacy and/or personal data. In this Deliverable, horizontal market segmentations are discussed as well as vertical relations observable in these markets.

Just like for cyber-security products, it is comparably difficult to define markets for personal information products and services. One stakeholder even labelled the task as 'slicing fog.' First and foremost, there is a great variety of terms: some use 'markets for electronic privacy', others 'markets for personal information' and still others speak of 'personal information management services' and/or 'privacy-enhancing technologies' (PETs) to describe the markets.

Secondly, privacy, i.e. the confidentiality and integrity of personal data, can emerge as part of an internal procedure of a company, a transaction quality or product trait (the reader is referred back to Figure 1 in this report). The sections below are therefore only a first step towards the development of a more comprehensive taxonomy of these markets. While in cyber-security markets, we can find hardware, software and services offers, all three seem to not exist in markets for personal data or privacy, see Table 3. Instead the players in the latter used hardware and cyber-security software and services as inputs to produce their outputs.

Table 3 Market Segments in Cyber-security and Privacy

Markets	Horizontal Market Segments		
	Hardware	Software	Services
Cyber-security	X	X	X
Privacy		X	X

Source: The author.

4.1 Horizontal Market Analysis

At the outset, it must be noted that the source of personal data, be it volunteered, observed or inferred, is always the data subject. However, the quality of identification of the respective person (i.e. the data subject) differs across market players and business models in these markets. For example, there are products that provide anonymity, i.e., non-identification and non-traceability of subjects. Firms with business models that vary (i.e., in the source of data) may compete in the same market segment. For example, a personal data vault differs a lot from a credit-reporting agency in terms of how the data are sourced, yet both could compete in identity verification provision services.

[20] Personal data in the context of this report is understood as defined by EU's Data Protection Directive 95/46/EC.

Market Definition and Relevant Players

Market Definition: The market for personal data and privacy can be defined as a physical or virtual place, where supply and demand for personal data and privacy goods and services meet.

Relevant Players: Players in these markets are companies, whose primary activity is related to the provision of software tools or services related to the digital identity of individuals. This means that the primary activity of the company generates most of its revenues in such software or services by either providing anonymization or pseudonymisation tools or by providing products and services that are based upon the collection and analysis of personal data.

According Crtl-Shift, a UK-based consultancy company, which focuses on consumer-direct products (where consumers are in control of data disclosure and usage), the market was in the past 5 years more considered to be something for start-up firms. However, now also large companies such as retailers increasingly understand the value-added that is provided to customers by offering new applications to them based upon their personal data. In addition, many companies start to realize that the old point of view on privacy is obsolete, where the data controlling rights are located at the firm collecting the information. Crtl-Shift states that companies can gain competitive advantage by putting the consumer in control of his/her data. The consultancy estimates that there are internationally about 400 companies active in its area of focus, i.e. where consumers have controlling rights over their data.

The market segmentation proposed in Figure 6 should be understood as an initial step in the process of finding better segmentation methods for this/these diverse market/s. Note that the below is a functional segmentation.[21]

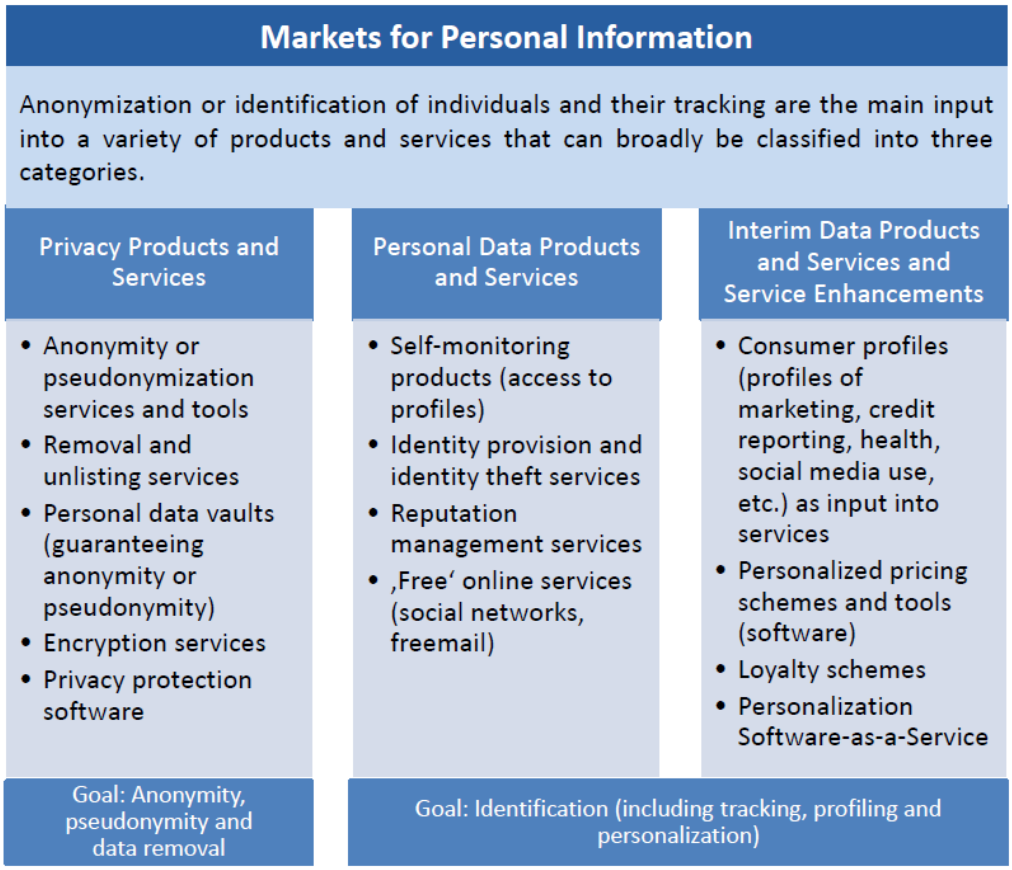
The **first category** captures software products and services that employ techniques of anonymization, pseudonymization, or encryption in order to provide privacy to the individual. Anonymity is the concealment of an individual's identity. Products that are directed at the consumer such as consumer-direct access and monitoring products fall into the **second category**. The **third category** consists of interim products and services as well as service enhancements. All three are discussed in greater detail below.

Firms may offer one specific tool or service, or, in some cases, they are active in several of the above segments by offering a portfolio or products and services. For example, the US- and UK-based credit-reporting agency Experian offers credit and marketing reports as well as self-monitoring products or services such as anonymity search engines as Ixquick.

Moreover, a portfolio of different *types of consumer information*, such as financial transactions and lifestyle information is likely to increase the possibility of a provider to offer one-stop-shop products and services.

[21] Products that serve the same goals can be seen as substitutes.

Figure 6 Personal Data and Privacy Market Scheme



Source: The author.

It should also be noted that the IPACSO project (Innovation Framework for Cyber-Security and **Privacy** Market Opportunities) only refers to **privacy markets, i.e. the first category in Figure 6.** However, for comprehensiveness, all three categories will be discussed.

4.1.1 PRIVACY PRODUCTS AND SERVICES

As previously noted, the first category in Figure 6 captures anonymization, pseudonymization or encryption tools and services. The guarantee of anonymity[22] or at least an increase in privacy by reduction of information disclosure is the primary purpose of these products and services. Examples are tools such as TOR, Eraser or Anonymizer as well as Silent Circle and Blackphone, the IXquick and Startpage search machines or personal data vaults that create a pseudonyms and do not show personal identity information to firms requesting information from the vault.

[22] Many IT-experts agree that there is no guarantee of 100% anonymity, if digital technologies are used. Thus, it is more apt to speak about 'quasi-anonymity.' However, for simplicity the world anonymity is used in this report.

4.1.2 Personal Data Products and Services

The second category captures products and services that are directly provided to the consumer and that are based upon the consumer's data (so-called 'consumer-direct products'). These products and services *do not* have the primary purpose of anonymization or pseudonymization. Instead an individual uses them for self-monitoring, reputation management or for a personalization of services. Examples are credit profile monitoring tools, identity theft, and reputation management services. Depending on who eventually owns the **information controlling rights**, these segments can be further sub-divided (not reflected in the Figure).

4.1.3 Interim Data Products and Services and Service Enhancements

Finally, in the third category, there are products that are not directly provided to the consumer or that constitute only an enhancement of another service, but still consist of the 'personal data resource'. Just as in the second category explained above, the provision of anonymity or increased privacy is not the primary purpose of these products and services, for which identification and monitoring is needed. For example, credit profiles and direct marketing or social network profiles are inputs into banking services or targeted advertising. In addition, personalized pricing is a service/product enhancement that does not involve the consumer as the 'manager' of the disclosure of personal data.[23]

4.1.4 Other Types of Market Segmentations

There are a number of other studies that have used different types of methodologies of segmenting the market for personal data products and services. It must be stated though that there are very few works in general. While some of the segments are fairly mature markets such as direct marketing and credit reporting, others are less than 10 years old, such as personal data vaults.

In the more mature market segments, there is on-going consolidation, which means that either company reports or competition cases in the relevant markets can be studied. However, these are not available for markets in which privacy products and services are sold. This is so because either the companies are start-ups, the products are in beta version only or the products are freely provided by networks of programmers or there were no relevant cases.

Market Segmentation in more mature personal data markets – There are a few competition cases in the consumer data markets of United Kingdom and Germany, which provide some basic information on market segmentations. For example, in the case of Acxiom Corporation's acquisition of Clarita Europe Group, the UK Office of Fair Trading reviewed the market for customer relationship management (CRM) services, which is part of direct marketing.[24] In the UK, the data collection component of CRM services can be further divided into list data, electoral roll, modelled and aggregated data and lifestyle data. The competition analysis mainly concentrated on the lifestyle data segment as relevant market.

[23] In fact, consumers are often unaware that they obtain personalized prices after disclosure of information.

[24] Office of Fair Trading (2004). Completed Acquisition of Acxiom Corporation of Clarita Europe Group, including Claritas (UK) Ltd.

In another case, the Office of Fair Trading divides CRM into the segments of data collection and sale, data analysis and database management.[25]

Another competition case occurred in in Germany, where Bertelsmann AG planned to create a joint company with InfoScore, a firm active in risk and debt management.[26] The authority stated that this move affected *two different markets*, one for debt and risk management (creditworthiness analysis) and one for direct marketing (address trading). These segments are reflected in the above classification scheme (Figure 6) in the third category (Interim Data Products and Services and Service Enhancements).

From a competition policy point of view, the question is whether an entity can control the supply of data, anti-competitively tie services, or use its market power in one or more segments of the supply chain to increase prices.[27] These questions need to be left open for future research with regards to these markets.

While these segmentations are recommendable for competition analysis, the dynamics in markets for personal data lead to a convergence of some segments and an alteration of others. Therefore, market segmentations need to adapt to the dynamically changing substitution relationships between products. For example, analysis of telecom data or social network data might allow inferences of creditworthiness, despite neither being traditional credit repayment data.

Market Segmentation in less mature personal data markets – The consultancy company Crtl-shift (2014: 31) focuses on information products where the consumer possesses controlling rights. The consultancy holds that such products transform the relationship between individuals and organizations. Three types of segments identified in this market are: (1) Personal Data Management; (2) Decision Support; and (3) Life Management.[28] The first type helps individuals to gather, store and analyse their own data. Example services are personal data vaults. The second enables individuals to collect and use information to make better individual decisions (such as price-comparison machines) and the third type enables individuals to use information to manage of life tasks and processes (such as moving homes).

4.2 Case Studies of Players in the Market for Personal Data and Privacy Products

Crtl-Shift: Crtl-Shift is a consultancy firm founded in 2009 and based in London, England, which is specialized in consultancy services in topics of the personal information economy. The consultancy provides advice to private sector clients (such as banks, telecoms or retailers) as well as authorities. It also publishes reports on the development of the personal data markets. In its consultancy services,

[25] Office of Fair Trading (2004). Anticipated acquisition by Acxiom Corporation of Consodata SA.

[26] Bundeskartellamt. Beschlussabteilung B9 – 32/05 (2005). http://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Fusionskontrolle/2005/B9-32-05.html

[27] Office of Fair Trading (2004). Completed Acquisition of Acxiom Corporation of Clarita Europe Group, including Claritas (UK) Ltd.

[28] An overview is provided in the infographic at: https://www.ctrl-shift.co.uk/news/2014/07/30/pims-infographic/

the company develops business models for information platforms, business propositions for prototype services or helps the government to develop strategies and metrics for specific programs that involve personal data. Crtl-Shift is a player that is only active in one segment (services) and wholly specializes on advisory, consultancy and research around the aforementioned topic.

Surfboard Holding B.V.: The Surfboard Holding B.V. is a for-profit company located in the Netherlands operating the websites Ixquick and Startpage. These websites do not collect personal data, and act as proxy between the user and Google (Startpage) or the user and the combination of a number of other search-related websites (Ixquick). As input the company purchases web searches (e.g. from Google) and produces as output a search service that is anonymized. The few web advertisements it shows are de-personalized. The users can choose to route their searches exclusively over servers in the U.S. or the Netherlands. It will now start a paid service providing email encryption (with StartMail.com). Moreover, the company uses mostly open source software and standard protocols to provide the best level of privacy given its resources. The company states that in the narrow field of anonymizing search engines, there are currently no real competitors in Europe.

SGP Technologies: SGP Technologies – a joint venture between the makers of Geeksphone and Silent Circle provides Blackphone, a smart phone that offers end-to-end secure communications. Featuring an operating system entitled PrivatOS, which provides a range of security options to improve the way users can manage their personal information, alongside Silent Circle's software, Blackphone provides a communications platform for both individual and enterprise use. The calls are routed over the IP network using peer to peer encryption. While the hardware is produced in Asia, real-time surveillance (by company staff and third-party quality control) is undertaken to ensure secure production of the phone. The firmware is digitally signed at the company's development offices before the manufacturing begins, allowing that signature to be verified on units coming off the line and ensuring no tampering has occurred. The company's data centers are located in Switzerland. The phone has been shipping since June 2014 and is bought by players in different industries, as well as governments and telecom carriers. The company expects to sell up to 10 million phones within the next three years, along with >50 million subscriptions to its Silent Suite of communications apps. One other competitor in the past in this field was FreedomPop.

For comprehensiveness, it should also be noted that there are other players that do not fit the proposed scheme, because they are neither a service provider, nor a software producer. For example, the Qiy Foundation, based in the Netherlands, is a non-profit company that provides an open standard for the exchange of personal attributes. This standard is licensed to users, including individuals and companies. It is currently in the developing phase, but will go live next year.

4.3 Supply Chains and Vertical Relations in Markets for Personal Data

In the following, a generic model of vertical relations in markets for personal data is provided. As explained earlier in this report, a supply chain connects production inputs with production outputs (see Figure 7). Production inputs are the data subject's disclosure of personal information as well as human capital, capital and buildings. Identity information is needed once products and services are provided that are based upon monitoring and tracking of individuals. Anonymity tools, on the other hand, do not require and thus do not collect identity information.

The outputs in personal data markets are primarily software tools and services. While for cyber-security offers the main goal is increased ICT security, the same holds for privacy, where the main goal is to establish, alter or retain a specific information distribution between relevant stakeholders with respect to personal data of the data subject.

Just as in cyber-security, there needs to be end-to-end privacy protection in the ***production of these goods*** as well as ***in their provision*** in order to obtain a secure product.[29] The same holds for the innovation processes in firms competing in these markets, where the ideas for new products are formed.

A peculiarity of markets for personal data and privacy products and services is that there are products based upon the input (identity information), but also based upon 'non-input' (anonymity). Although in many cases, the two types of products are marketed by using 'privacy' as selling point. The provision of anonymity products increases customer choice, where there is commonly a stigma associated with the use of privacy technologies. This social stigma could be one of the reasons, why this market does not work well yet. As of 2014, however, there seems to be somewhat of a change of mind, because some companies now have started to equip their employees with technologies that are not easy to compromise and that increase the cost of eavesdropping and decryption.

Another key aspect is that the legal consent regime frames the value chain and frequently gives rise to shared ownership rights, where the consumer and the information-collecting firm co-own the data. Individuals either grant consent directly or allow a company to disclose personal data to a third party on their behalf (see dashed line in Figure 7).[30]

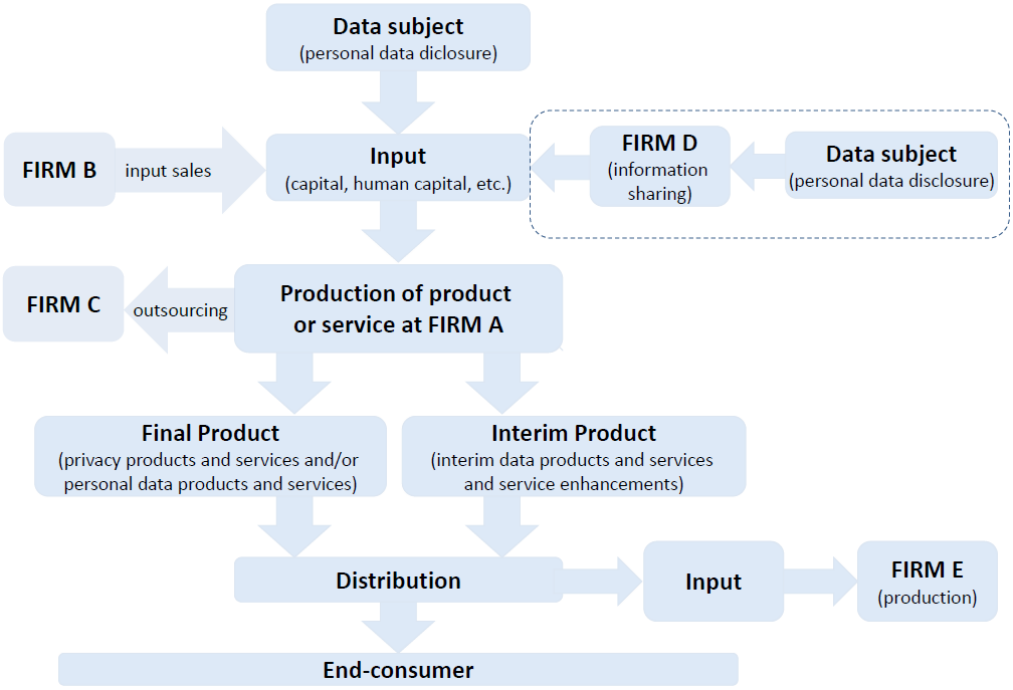
Data products and services might be either directly sold back to the data subject or are used by downstream industries as inputs into their own production processes (see the aforementioned Figure 6). Examples for downstream industries range from the banking industry to telecommunication firms or retailers, to name a few. Moreover, personal data processors can engage in cross-licensing or re-selling of their data assets.[31] It is important to note that at the production stage, there are also outsourcing relationships in case of data analysis, for example, or input purchases.

Figure 7 Supply Chain in Personal Data Markets

[29] In this context, privacy protection encompasses the technical security of personal information as well as procedures and business practices that minimize risks of unauthorized access to the data.

[30] This is the so-called opt-in regime. In the opt-out regime third-party information sharing needs to be actively stopped by the data subject.

[31] In cross-licensing, Firm A licenses the use of data by Firm B that in turn pays Firm A share of the revenue obtained from data use and sale.

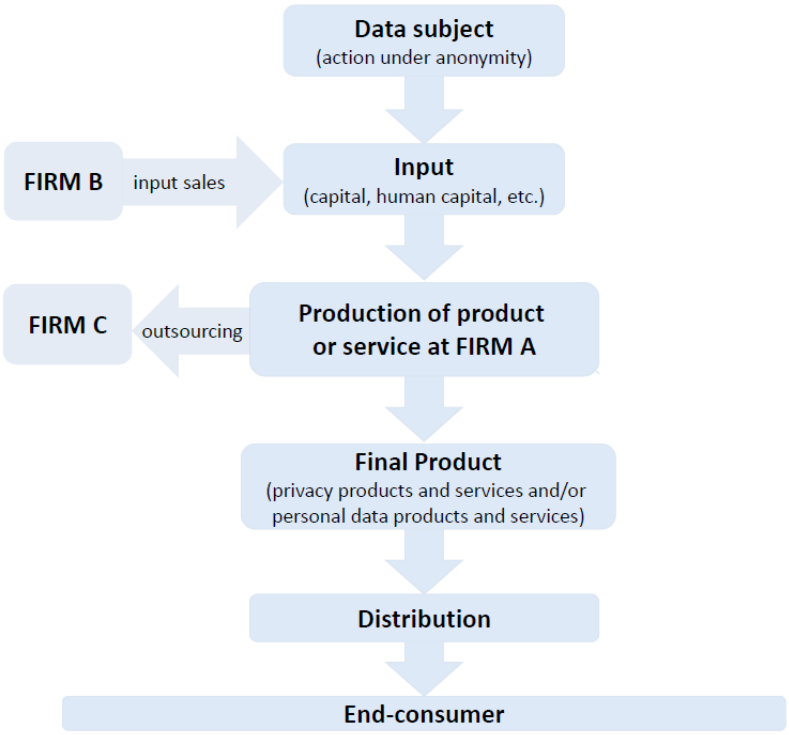


Source: The author.

There are, of course, important differences with respect to the value chain that arises (again, it is only a very general model) with respect to provision of anonymity services (see Figure 8). In this case, there is no input of personal data, but an action of the user under conditions of anonymity. Again, no 100% anonymity can be guarantee, but the costs of re-identification are increased with the products. Examples are the Startpage and Ixquick search machines, which do not record IP numbers. They are described as case studies in this report.

While many of the products and services discussed here are final products, one example, of an interim privacy product is PrivatOS, the operating system used in the Blackphone (see case studies). This operating system provides encryption for phone calls, emails, texts, and internet browsing.

Figure 8 Supply Chain in Privacy Products and Services



Source: The author.

It is important to note that also here, end-to-end privacy can only be established by securing the supply chain. One example of insecure input is the Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG) published by the National Institute of Standards and Technology (NIST). It is reported that the Snowden revelations showed that "the National Security Agency used its influence over NIST to insert a backdoor into Dual_EC_DRBG and possibly weaken other cryptographic standards."[32] These standards where used in many appliances, once of them being the Blackphone.[33] For the latter, the managers decided to use a non-NIST cipher suite in future. This is one example, how a compromised or weakened input into a vertical chain endangers the final output, namely the promise of increased privacy.

4.4 Vertical Relations with the Cyber-Security Industry

As an end-user of ICT security products, the personal data and privacy industry is located downstream from the cyber-security industry. For example, the U.S.-based credit-reporting agency TransUnion uses Oracle Databases and Encryption technologies to meet Payment Card Industry Data

[32] PC World (2014). Overreliance on the NSA led to weak crypto standard, July 15, 2014, http://www.pcworld.com/article/2454380/overreliance-on-the-nsa-led-to-weak-crypto-standard-nist-advisers-find.html

[33] See the Silent Circle Blog: https://blog.silentcircle.com/nncs/.

Security Standards. The German credit reporting agency Schufa uses Oracle databases. Large IT-companies also partner with information providers in order to supply clients with specific tools.[34] Further, some IT corporations have outsourced the management of collected personal identifiable information to third parties. For example, Symantec processed payment information of customers through a call center in India, where the data was compromised.[35] Symantec is a relevant player in the service segment of the cyber-security market. Accordingly, there are inter-linkages between the cyber-security industry and the personal data industry: the latter purchases products from the former and both cooperates in joint product/service provision.

V. Economic Incentive Templates

One goal of the IPACSO project is to develop economic incentive templates that feed into the Innovation Framework, becoming a knowledge generator enabling innovators to better understand the opportunities in the market. **Annexes 1-3** present the templates that can be used by innovators, but also other stakeholder such as policy-makers in the assessment of cyber-security and privacy markets.

In order to further **market opportunities**, the templates can be used for:

- Market sizing and segmentation and trend analysis;
- Competition analysis and analysis of operating environment;
- Comparisons of market segments; and
- Understanding of vertical relationships.

The templates enable a more holistic picture about markets that are currently rather undefined in Europe. The horizontal mapping gives a view of the general landscape and what players belong to the market of cyber-security and privacy.

Table 4 Economic Incentive Templates for Assessing Market Opportunities

Template	Explanation
Mapping of market (horizontal analysis)	The horizontal analysis of the cyber-security and privacy market involves the definition as well as the segmentation of the market.
Mapping of competition (horizontal analysis)	The competition analysis includes an analysis of the threat of entry, potential substitutes, bargaining power of relevant players (i.e. dominant buyers) and rivalry between suppliers. This is a necessary assessment for the analysis of cyber security and privacy market opportunities.
Mapping of value chain (vertical analysis)	The vertical analysis of cyber-security and privacy market involves the mapping of upstream and downstream players relevant for the IPACSO innovator.

Source: The author.

[34] For example, SAP and Experian Data Quality partner in order to supply SAP clients with Experian's off-the-shelf quality tools.

[35] Leyden, J. (2009). Indian call centre credit card 'scam' exposed - Symantec renewal details end up on black market, http://www.theregister.co.uk/2009/03/20/call_centre_credit_card_fraud/

The competition mapping informs about important subjects that enable competition and could be a threat to a young company. Further the mapping of the value chain enables an understanding of the vertical relationships that exist in cyber-security and privacy markets as well as the potential dependencies, cyber-security threats and privacy risks that lurk in these relations.

VI. Conclusions

At this stage, there are only scattered works on the market for cyber-security goods and services, only one work on the market for personal data goods and no analyses on vertical relations in cyber-security and privacy markets. This limited availability inhibits market analysis and trend forecasting in order to assess market opportunities. It limits the understanding of what types of competitive forces shape the market, what segments grow or decline, what players enter and exist and where new opportunities for cyber-security and privacy innovation exist.

This **IPACSO WP4 Deliverable – D4.2** feeds into the overall IPACSO Framework by providing knowledge on horizontal as well as vertical assessments of markets and market relationships. It is based upon stakeholder interviews as well as desk research.

It explains the challenge of assessing these markets, compiles different market segmentation approaches and explains vertical relationships. It also points to the fact that deep integration of supply chains increases certain risks such as linkage attacks. This must be extended to the innovation stage. Moreover, a key takeaway is the rule of secure procedures in the development of cyber-security products and end-to-end privacy rules in the production of personal tools and software. Moreover, the report not only discusses the difference between the market for cyber-security and privacy, but also the linkages that exist between both.

The deliverable also develops a Privacy and Cyber-Security Innovation Value chain that connects inputs to outputs in the production of innovation.

Based upon this work, different types of economic incentive schemes are presented to further adoption of privacy and cyber-security technologies at the industry-and firm-level. In order to also become a knowledge generator for innovators, different economic incentive templates are developed that enable the assessment of market opportunities. These will be applied and further developed in D4.3.

List of References

Bundesministerium für Wirtschaft und Technologie (2013). Der IT-Sicherheitsmarkt in Deutschland Grundstein für eine makroökonomische Erfassung der Branche, Berlin, http://www.Bundesministerium für Wirtschaft und Technologie.de/DE/Mediathek/publikationen,did=585290.html.

Ctrl-Shift (2014). Personal Data Management Services: An Analysis of an Emerging Market, https://www.ctrl-shift.co.uk/research/product/90.

Hansen, M.T. and J. Birkinshaw (2007). Innovation value chain, Harvard Business Review (June), http://hbr.org/2007/06/the-innovation-value-chain/ar/

IDC EMEA (2009). The European Network and Information Security Market - Scenario, Trends and Challenges, A study for the European Commission, DG Information Society and Media, Final Study Report, April.

Micromarketmonitor (2014). Europe Cyber Security Market, Report CY 1000, publication date: 28.9.2014, http://www.micromarketmonitor.com/market/western-europe-cyber-security-4129808188.html.

NIS Platform Working Group 3 (2014). State-of-the-Art of Secure ICT Landscape (Draft Version), http://ecrime-project.eu/wp-content/uploads/2014/05/TSI-Report-State-of-the-art-of-secure-ICT-landscape.pdf

PAC (2013) Competitive analysis of the UK cyber security sector – A study by Pierre Audoin Consultants for the Department for Business, Innovation and Skills, Version 1, July 29th, 2013.

Porter, M. (1979). How Competitive Forces Shape Strategy, Harvard Business Review, March/April 1979.

UK Trace & Investment (2012). Cyber Security – The UK's Approach to exports, http://www.gchq.gov.uk/press_and_media/news_and_features/Documents/Cyber_Security-the_UKs_approach_to_exports.pdf

Feldfunktion geändert

ANNEX 1

Economic Incentives Template for Horizontal Market Analysis	
This IPACSO Template is supposed to serve as a guideline for analysis of the market an entrepreneur would like to enter with a new product or service. A companion publication is the Output D4.2 of the IPACSO project.	
Indicator	**Explanation**
Market entry conditions	What types of market entry barriers do exist (large start-up costs, licensing & certification, etc.?)
Main competitors	Who are the main competitors with very similar products, if they exist? Is the market highly concentrated?
Potential competitors	Who are potential future competitors and is it easy to integrate the technical solution into off-the-shelf products that already exist? Does competition from abroad exist?
Behaviour of relevant competitors?	What can be learnt from a competitors behaviour in the past (pricing strategy, innovation capacity, etc.)?
What are the competitor's product strategies?	What product strategy does the competitor or potential competitor employ (personalization, customization, product packaging)?
Who generates the demand?	Who are the main customers of the product: firms (Large, SMEs, etc.), government or consumers?
How is the demand side segmented?	How can similar groups of consumers be clustered? Are some of them having the same privacy and/or security products?
What interdependencies between players exist?	Are there any cooperation, supplier-demander relationships, marketing partnerships, etc. among the (potential) rivals that are relevant?
Are products differentiated?	Are the competitor's products differentiated or personalized in order to have it tailored to the customers' needs
What types of prices are set?	Are there specific price-setting schemes (such as fixed-fees, subscriptions, licensing-fees, personalized prices, etc.)

ANNEX 2

Economic Incentives Template for Operating Environment	
This IPACSO Template is supposed to serve as a guideline for analysis of the market an entrepreneur would like to enter with a new product or service. A companion publication is the Output D5.1 of the IPACSO project.	
Indicator	**Explanation**
Threat of entry	Some key factors which may increase the threat of entry are profitability, which does not require economies of scale, brand names that are not well-known, or initial capital investment that is low. Other factors are low consumer switching costs, as well as proprietary technology or materials that are not an issue.
Substitutes	Consumer switching costs are low, substitute product is cheaper than industry product, substitute product quality is equal or superior to industry product quality, substitute performance is equal or superior to industry product performance
Bargaining power of buyers	Bargaining power increases if buyers are more concentrated than sellers, buyer switching costs are low, threat of backward integration is high, buyer is price sensitive, buyer is well-educated regarding the product, buyer purchases product in high volume, buyer purchases comprise large portion of seller sales, product is undifferentiated, and if substitutes are available
Bargaining power of suppliers	Bargaining power of suppliers is high if suppliers are more concentrated than buyers, buyer switching costs are high, suppliers can easily integrate forward (i.e. start producing the buyer's product themselves), the buyer is uneducated regarding the product, the supplier's product is highly differentiated, the buyer does not represent a large portion of the supplier's sales, and if substitute products are unavailable

This is quote from IPACSO Deliverable 5.1 based upon Porter (1979).

ANNEX 3

Economic Incentives Template for Vertical Analysis	
This IPACSO Template is supposed to serve as a guideline for analysis of the market an entrepreneur would like to enter with a new product or service. A companion publication is the Output D4.2 of the IPACSO project.	
Indicator	**Explanation**
What are the main inputs needed into the own production process?	Main input categories are: capital (hardware, software, buildings), human capital (R&D, MINT skills), etc.
Technological integration?	Is there vertical technological integration needed with other firms' products or services? Is the own product/service platform dependent or independent?
Adjacent supply chains?	Are there any products/services that must be purchased from others during the process of delivery in order to be able to provide the good or service?
Distribution to end-users?	What kind of distribution network is needed in order to bring the product to the end-user?
Customer feed-back cycle?	What are the feedback mechanisms in order to integrate customer opinions and suggestions?
Output - final products or interim product?	Who are the final consumers or the product and if the product is interim input into another firms production, who are the customers of those firms?