

Business Cases and Innovation Paths

NIS PLATFORM

WORKING GROUP 3 (WG3)

FINAL, Version 1.1

May, 2015

Editors:

Paul Kearney (BT)

Zeta Dooly (TSSG, WIT)

Executive Summary

This report is a deliverable of Working Group 3 (WG3) of the EC Network and Information Security (NIS) Platform. It feeds into the main output of WG3, a Strategic Research Agenda (SRA) for cybersecurity in Europe using 2025 as the time horizon.

The availability of new and improved NIS products and services will benefit the European economy in three main ways:

- By reducing the cost to European organisations and individuals arising from security breaches and related incidents;
- By addressing the risks (real and perceived) associated with new technologies and practices. Many people and organisations are reluctant to introduce potentially valuable innovations because of concerns over security. Enabling them to be used securely, allows the benefits to be realised.
- Increased revenue generated for European companies from new products and services, and the employment generated from growth in established businesses and creation of new companies.

This report complements the other WG3 deliverables by looking at the SRA from a market-oriented perspective in order to gain insight into:

- a) The key aspects of demand for NIS innovation so as to ensure NIS research is focused on challenges achievement of which would have the greatest impact;
- b) Research & Innovation (R&I) models and processes that are most efficient and effective in bringing usable, affordable and timely solutions to market.

NIS has a number of characteristics that demand special consideration from an R&I point of view. Firstly, NIS involves combat with an intelligent foe; rather than being about solving a static problem, it is an adversarial 'game' between attack (bad) and defence (good). On a tactical level, the 'game' is about preventing and responding to attacks, while on a strategic level it is about co-evolution of tools and tactics. This makes the future threat environment highly dynamic and extremely difficult to predict. In consequence, future NIS solutions will need be continuously evolvable in order to establish and maintain a lead over the threat without leaving windows of vulnerability. Furthermore, the number, diversity, organisation, persistence and sophistication of threat agents facing the defender is continually growing, with some having a high degree of expertise, organisation, motivation, persistence and financial and political backing. Even amateur threat agents have easy access to powerful, automated attack tools. Currently, threat agents have the upper hand, so our aim must be not only to maintain the status quo regarding security risk exposure, but to gain the initiative from them.

Secondly, an attacker will probe defences to find and exploit any weak link. Thus, NIS solutions must be recognised as complex human-technical systems consisting of many dissimilar elements that must work together harmoniously. Consequently they require a holistic approach. Currently, technical security measures are largely used independently, with people providing the matrix that integrates the components. In the future, the pace of response required means that the technical systems will need to co-operate directly. This has implications for the dynamics of

innovation as it is more difficult for a radically different approach to penetrate the market due to the need for a new product or service to be compatible with the existing elements with which it must interact.

Thirdly, NIS is not a technology itself, but a mind-set and a collection of principles that must be applied in a technical and organisational/social context. The pace of innovation in technology and in the business practices, leisure activities and societal institutions that exploit it, means that NIS must re-invent itself continuously. It is straightforward to list current technical and process innovations that are problematic conventional security approaches (Cloud, Internet of Things, Mobility, etc.) and we can be sure that the years between now and 2025 will bring further challenges. While the specific innovations are difficult to anticipate, it is probable that the trends of increasing technological diversity, ubiquity, interconnectivity, complexity, shared usage and interdependence will result in a global, common, ICT infrastructure that is critical to society and the world economy, and which is likely to remain vulnerable to attack.

Finally, NIS must serve the needs of European society as reflected in public opinion, government policy, and legal and regulatory frameworks, and must do so in a transparent and accountable way. However the wishes of society are a dynamic equilibrium of inherently conflicting drivers, with the balance point affected by many factors including events, such as terrorist attacks, leaks of personal data, and revelations about government surveillance programmes. This results in a fragmented and unstable legal/regulatory/oversight environment.

The most fundamental requirement for an effective market (or set of markets) in NIS is the establishment of a true engineering science of secure and trustworthy systems. While it will be important to include development of trusted hardware and software elements (i.e. ones that have well-defined security properties and are largely free of errors and vulnerabilities) as one discipline within the science, the main emphasis will be on the analysis, design and operation of dynamic systems and the understanding and prediction of their properties. This is needed to allow the reliable construction of solutions that satisfy the requirements of demand-side stakeholders in the face of the prevailing threat. In general, such solutions will combine people, processes and technology, so the science will need to encompass an understanding of (benign and malicious) human behaviour and how to influence it, as well how to combine human and technical elements harmoniously and synergistically. Although people will remain an important part of the solutions, the shrinking window for timely response to attacks make an increasing degree of autonomous operation of technical controls essential. People will set policies enacted by autonomous controls, monitor their operational effectiveness and adapt them as required.

Such systems occur on multiple levels, and it should be possible to reason about, e.g. the federation of NIS systems to support co-operation among enterprises, law enforcement agencies, and national and European authorities. At any compositional level, it should be possible to define meaningful risk metrics that can be calculated operationally to allow continuous monitoring, and also policy-based means of influencing system behaviour in a predictable way. Such mechanisms to assert rights and enforce transparency and accountability should be available to all legitimate stakeholders in the system.

In a mature market for NIS, a customer (either an end-customer or an intermediary in the value chain) seeking an element to play a particular role in a system should be able to choose among several comparable alternative products and services from different providers. While these may differ in price, implementation, technology and effectiveness, they should essentially be substitutable one for another. Similarly, products and services from different providers that play complementary roles within a system should be compatible and interoperate with each other. If this is not the case, the scope for innovation is limited. Stimulating and fostering the emergence of an understanding of sets of abstract product/service roles that can be combined in various ways to satisfy NIS requirements, is therefore an important aspect of an SRA.

We have proposed a methodology designed to elicit sets of NIS capabilities, as we term such abstract roles. The approach is based on defining and analysing a representative selection of demanding use case scenarios. In each case, demand-side stakeholders of three types are identified: process owners, process participants, and regulators (concerned with wider organisational or societal issues), and their security objectives and concerns in that scenario described. A collection of future security services that would meet their requirements is then hypothesised. The future service concepts resulting from the scenarios are then correlated and generalised to produce a number of sets of compatible security capabilities.

We envisage that the abstract capabilities will be to a large extent timeless, though the 'technologies' required to realise them effectively depend on the threat environment, prevalent technologies and 'business' processes, and socio-political factors time applicable to a given time horizon - those required in 2025 will be radically different from today's best practice. The idea is that research investment can be targeted at those technologies that will make the biggest difference overall, taking into account that some technologies will advance the state of the art across multiple capabilities and scenarios, while others may deliver significant benefit a few key applications. We have selected and begun working through a few example scenarios to illustrate the approach. We intend that aspects of the approach will influence the SRA, but applying it fully is beyond the scope of WG3. We believe the methodology has merit, however, and should be considered for use in a longer-term roadmapping activity to extend and maintain the SRA.

Innovation begins when developers or service providers identify an opportunity to address a need (which may not yet be recognised by customers) in a new and better way. They must then implement a product and bring it to market. Ideally, in a truly competitive market, a product that is genuinely better or more attractive would succeed. In the language used above, an innovative product or service would exploit a new technology to implement an improvement to a capability. Since capabilities are often interdependent, the success of an innovation may depend on compatible innovations occurring in adjacent capabilities. Thus, the existence of dependencies may both hinder and stimulate innovation. Occasionally, a paradigm shift will occur resulting in the emergence of a new capability set, but this is relatively rare. Innovation will depend on research to provide new enabling technologies, but the two types of process operate on different timescales, require different skills and are often carried out by different communities of people.

Alignment and efficient coupling of research and innovation sub-processes are therefore critical to the success of the overall R&I process.

We have reviewed R&I process models in use in WG3 member organisations and reported in academic papers in order to establish a picture of current practice. Most espouse variants of Open Innovation, whereby the R&I value chain is enacted by an open ecosystem of small and large enterprises, individual inventors, research institutes and universities. Large enterprises are experimenting with a variety of schemes to stimulate and benefit from entrepreneurial activities outside their organisations. Similarly, national and EU research programmes are trying out new instruments designed to encourage participation by small companies and to grow this sector of the market. Information gathering and analysis is still in progress, but it appears that while the general philosophy of Open Innovation is shared, there is considerable variation in how it is interpreted and applied, and a consensus on best practice has yet to emerge.

A main message emerging from the work is that NIS R&I needs to be approached holistically. One aspect of this is that R&I activities need to co-ordinated actively to ensure that results from groups of projects can be used in combination to construct the NIS solutions needed by the market. However, top-down imposition of a rigid framework will stifle innovation and fail to deliver the desired results. Instead, we advocate a more evolutionary approach in which divergent tendencies generated by bottom-up independent research are countered by top-down convergent forces resulting in the emergence of more dynamic structural relationships.

The scenario-based approach taken in parts of this report can be seen as an example of this philosophy, in which analysis of scenario-specific requirements interacts with research topics and a process of abstraction to generate R&I roadmaps structured in terms of sets of compatible abstract capabilities. One proposal is that this approach be adopted by an existing Horizon 2020 Co-ordination and Support Action (CSA), or provide the basis for a new one. The idea is that scenarios managed by the CSA would provide application contexts against which concrete capability instances developed by different projects could be evaluated in combination. The CSA would provide a convergent force to align the directions of projects and encourage compatibility of results.

A related idea is to fund the establishment of experimental testbeds / innovation incubators with access to real data and simulated threat and application scenarios. These would be shared resources accessible to a wide range of stakeholders and would support research, innovation and validation. Cross-project experimental prototyping would be strongly encouraged, or even strictly required. The testbed environments themselves could act as prototypes for innovation-friendly operational platforms.

These and other recommendations are summarised at the end of the main body of the report.

Business Cases and Innovation Paths

Table of Contents

1	Introduction and problem definition	11
1.1	Introduction	11
1.2	Background	11
1.3	Problem definition and analysis	13
1.4	Structure of the report	16
2	Economic benefits of NIS research and innovation	18
2.1	Reducing the cost of security breaches	18
2.2	Reducing the risk of innovation	19
2.3	Growing the European NIS product and services sector	22
2.3.1	How big is the global NIS market?	22
2.3.2	NIS Market Size and Growth By Region	24
2.3.3	Market Size and Growth By NIS Product/Solution Categories	25
2.3.4	EU NIS market strengths and weaknesses	27
3	Market and Industry overview	29
3.1	Introduction	29
3.2	Horizontal and vertical market analysis	31
3.3	Global technology vendors	34
3.4	The European Solutions for Cybersecurity	34
3.4.1	SWOT Analysis	35
3.4.2	Strengths	35
3.4.3	Weaknesses	35
3.4.4	Opportunities	36
3.4.5	Threats	36
3.5	Conclusion	36
4	An approach to prioritising research topics	38
4.1	Stakeholders and requirements	39
4.1.1	Demand-side stakeholders	39
4.1.2	Innovation Stakeholders	44
4.2	Approach to cost-benefit analysis of research topics	47
4.3	Market demand and high impact use cases	50
4.4	Example research topics and value statements	51
4.5	Next steps	51
5	Process Definition & Innovation Models	52
5.1	Introduction	52
5.2	Contextual considerations	54
5.3	Innovation Models	54
5.3.1	First Generation- Technology Push (1950s to mid 1960s)	56
5.3.2	Second Generation – Market Pull (Mid 1960s to early 1970s)	57
5.3.3	Third Generation – Interactive, Coupling or Chain-linked models (Early 1970s to mid 1980s)	57
5.3.4	Fourth Generation – Integrated model (Early 1980s to early 1990s)	57
5.3.5	Fifth Generation – Systems integration and network model	58

5.3.6	Sixth Generation Open Innovation Models	58
5.3.7	Conclusion	59
5.4	European and US approaches to innovation in technology.....	59
5.4.1	Research and Innovation in BT	60
5.4.2	Research and Innovation in Engineering Ingegneria Informatica S.p.a (ENG) 61	
5.4.3	Research and Innovation in Espion.....	63
5.4.4	Research and Innovation in ATOS Research & Innovation (ARI)	64
5.4.5	Research and Innovation at HP	68
5.4.6	Research and Innovation at SAP.....	72
5.4.7	Research and Innovation at Technikon	73
5.4.8	Research and Innovation with Industry Clusters – example LSEC – Leaders In Security.....	74
5.5	Initial Research & Innovation Analysis	77
5.6	Economic analysis and the focus on incentives.....	78
5.6.1	Introduction to Economic Incentives.....	79
5.6.2	Conclusion	80
5.7	Recommendations to H2020 on innovation processes	81
5.7.1	Keys to speed up the process and success	82
5.7.2	Improving prospects of success.....	83
5.7.3	Best practice	84
6	Summary of recommendations	86
6.1	Input to the NIS Strategic Research Agenda.....	86
6.2	Stimulating and promoting innovation.....	88
6.2.1	Keys to speed up the process and success	89
6.2.2	Improving prospects of success.....	90
6.3	Total NIS R&I.....	90
Appendix A	Summaries of source documents	93
A.1	Pierre Audoin Report for the UK Department of Business, Innovation and Skills 93	
A.2	CAPITAL - Cybersecurity research Agenda for Privacy and Technology challenges.....	94
A.3	Innovation organisations in EU member states.....	95
A.3.1	Italy.....	95
A.3.2	Spain	96
A.3.3	UK	97
Appendix B	United States example of R&D Execution model	99
Appendix C	EIT institute and its “EIT ICT labs” Knowledge Innovation Community (KIC):.....	102
Appendix D	Success stories in European NIS innovation	105
D.1	NIS innovation success stories at BT.....	105
D.1.1	BT Assure Analytics.....	105
D.1.2	Security capabilities for BT Cloud Compute platform	106
D.2	Security innovation awards and recognition	106
D.2.1	EY Startup Challenge	106
D.2.2	British Computer Society UK IT Industry Awards,	107
D.2.3	SC Magazine Awards Europe	107

D.2.4	Computing Security Awards	108
D.2.5	Deloitte Technology awards	108
D.2.6	Gartner Cool Vendors in Security for TSP	108
D.3	IPACSO innovation awards - Research and Innovation in Sedicii.....	109
Appendix E High impact use cases: examples from applying the methodology 112		
E.1	Security for Internet-of-Things Infrastructures.....	112
E.1.1	Description of setting	112
E.1.2	Dramatis personae	113
E.1.3	Main security concerns of stakeholders.....	113
E.1.4	New services that would solve the problem	113
E.2	Advanced infrastructures for supporting secure and privacy-preserving data management and governance at scale.....	114
E.2.1	Description of setting	114
E.2.2	Dramatis personae	115
E.2.3	Main security concerns of stakeholders.....	115
E.2.4	New services that would solve the problem	116
E.2.5	Required enabling technologies / capabilities.....	116
E.2.6	Assumptions/Dependencies.....	117
E.3	Data Business: Data becoming the major business asset and the foundation of new businesses.....	117
E.3.1	Description of setting	117
E.3.2	Dramatis personae	118
E.3.3	New services that would solve the problem, and required enabling technologies.....	118
E.3.4	Assumptions/Dependencies.....	119
E.4	Stealthy industrial espionage by APT.....	119
E.4.1	Description of setting	119
E.4.2	Dramatis personae	120
E.4.3	New services that would solve the problem	120
E.4.4	Required enabling technologies / capabilities.....	121
E.4.5	Assumptions/Dependencies.....	121
E.5	The Insider Threat.....	122
E.5.1	Description of setting	122
E.5.2	Dramatis personae	123
E.5.3	Main security concerns of stakeholders.....	123
E.5.4	New services that would solve the problem	123
E.6	Effectiveness of security controls mitigating IT risks: From qualitative to quantitative benchmarking	124
E.6.1	Description of setting	124
E.6.2	Dramatis personae	124
E.6.3	New services that would solve the problem	124
E.6.4	Required enabling technologies / capabilities.....	127
E.6.5	Assumptions/Dependencies.....	127
Appendix F Example research topics and value statements		
F.1	Security services and capabilities	128
F.1.1	Trusted Identity Service.....	128
F.2	Trusted and resilient infrastructure.....	130

F.2.1	Trusted Service Infrastructure	130
F.2.2	Low-cost Security for Internet-of-Things Infrastructures (Matthias)	131
F.3	Secure Engineering (Tools and Methodologies)	131
F.3.1	Risk-driven secure engineering of critical enterprise systems	131
F.4	Security management solutions	131
F.4.1	Managed operational security for SMEs	131
F.4.2	Quantitative Benchmarking of IT Security Controls	132

Contributors to the deliverable include:

- Aljosa Pasic, ATOS Origin
- Erkuden Rios, Tecnia
- Dharmendra Kapletia, HP
- Gérard Gaudin, Club R2GS
- Klaus-Michael Koch, Technikon
- Mari Kert, EOS
- Matthias Schunter, Claire Vishik, Intel
- Nicola Jentzsch, DIW Berlin
- Okonweze Austen, UK Department of Business, Innovation and Skills (BIS)
- Paul Kearney, BT
- Riccardo Zanetti, Veronique Pevtschin, Engineering Group (Eng)
- Seamus Galvin, Espion Group
- Ulrich Seldeslacht, LSEC
- Volkmar Lotz, SAP
- Zeta Dooly, Jamie Power, TSSG, Waterford Institute of Technology

Contributing Projects:

This document has been prepared with the support of the following EU projects:
IPACSO, CAPITAL, SecCord, FIRE.

1 Introduction and problem definition

1.1 Introduction

Much of European social, commercial and governmental activity is already critically dependent on Information and Communication Technologies (ICT), and we can only expect that dependence to continue to grow for the foreseeable future. Unfortunately, despite efforts to improve the quality and resilience of ICT systems, these remain vulnerable to attack. Furthermore, recent years have witnessed the proliferation and diversification of classes of threat agent that are able and willing to exploit such vulnerabilities for a variety of motives causing significant adverse impact in the process.

The scale of the challenge and its significance to European society clearly merit research investment at the EU and national levels and also. Moreover, while European companies will benefit commercially from improved cybersecurity techniques, technology and services, the research investment and scope is beyond the means of individual enterprises. A co-ordinated approach is required to ensure a healthy ecosystem of providers of compatible products and services, and a competitive market to drive innovation. In addition to improvements in cybersecurity, European society will benefit from a vibrant and dynamic indigenous industry able to address global markets.

Experience has shown that providing research funding, and selection and governance mechanisms, while necessary, is not sufficient to ensure the desired research and innovation outcomes. Even where projects succeed in advancing the state of the art in an area relevant to important security challenges, this does not necessarily mean that the results will be taken up and applied by technology and service providers and end-users.

The purpose of this report is to improve the success rate of research projects in achieving impact on major cybersecurity challenges and enhancing the competitive position of Europe's cybersecurity industry

1.2 Background

This report is a deliverable of Working Group 3 (WG3) of the EC Network and Information Security (NIS) Platform.

The NIS Platform was established by DG CONNECT in response in a call for *“for the establishment of a platform, bringing together relevant European public and private stakeholders, to identify good cybersecurity practices across the value chain and create the favourable market conditions for the development and adoption of secure ICT solutions”* Cybersecurity Strategy of the European Union¹. It is intended

¹ Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN/2013/01 final

to complement and underpin the EU NIS Directive, and to provide input to the secure ICT Research & Innovation agenda at national and EU level, including the Horizon 2020 programme. The launch meeting was held in Brussels in June 2013, and resulted, amongst other things, in the creation of three working groups:

1. risk management, including information assurance, risks metrics and awareness raising;
2. information exchange and incident coordination, including incident reporting and risks metrics for the purpose of information exchange;
3. secure ICT research and innovation.

Each working group was to have two chairs, one each from the public and private sectors.

The main output of WG3 is to be the Strategic Research Agenda (SRA) of the NIS Platform. This is intended to be a living document using other WG3 deliverables as input, specifically:

- Secure ICT landscape
- Snapshot of Education & Training landscape for workforce development
- Business Cases and Innovation Paths (this document)

In addition, work is proceeding directly towards the SRA, organised according to three so-called Areas of Interest (Aoi), with the provisional titles of 'Citizen Digital Rights and Capabilities' (looking at cybersecurity from an individual perspective) Resilient Digital Civilisation (taking a collective/societal perspective) and 'Trustworthy Hyper-connected Infrastructures' (looking at the secure and resilient infrastructure required to enable the other two perspectives). A first consolidated version of the SRA is due in March 2015.

1.3 Problem definition and analysis

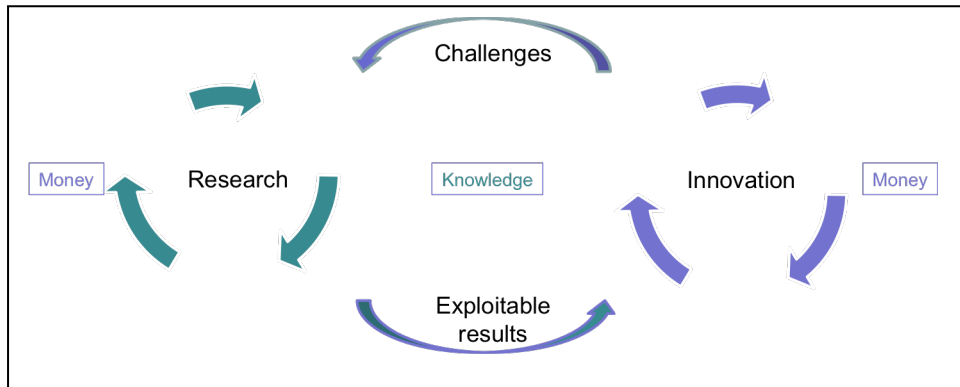


Figure 1: Research and Innovation as coupled parallel processes

Research and innovation are distinct, but related, processes that must combine harmoniously if significant positive impact on society is to be realised. Research is concerned with generating new knowledge. In disciplines such as the ‘pure’ sciences, arts and humanities, research results may have purely cultural value. However, in engineering, applied science and similar disciplines, research results should at least have the potential to contribute to or influence some beneficial change to the way the world works. Actually utilising new knowledge to achieve such changes is the role of Innovation.

There are a number of valid reasons for treating research and innovation as separate processes within the overall transformational value chain:

- Research and innovation projects require different mixes of motivations, skills and abilities that are not often found in the same individuals;
- They are often carried out in separate organisations. Even in large enterprises where both activities occur, they are frequently the responsibility of different departments;
- They are often funded by different bodies or at least from different budgets;
- They operate on different characteristic timescales, e.g. 2-5 years for research projects and 3-6 months for innovation projects.

This last point is one major reason why research and innovation should be regarded as communicating parallel processes rather than steps in a linear pipeline. Another is that the relationship between research results and innovation results is not one-to-one; research results are comparatively generic, so that a given significant result can be applied in different ways to deliver innovations in multiple problem domains. Finally, there needs to be two-way communication between research and innovation processes. As well as research supplying innovation with new exploitable knowledge, innovation must provide information on outstanding requirements and challenges to guide/adapt the direction of future research.

If we accept this, admittedly simplistic, model of research and innovation, we can identify three main failure modes:

1. Research fails to provide new knowledge that can provide the basis of innovation (e.g. because projects failed to provide new knowledge, because the new knowledge was not relevant to real-world problems, or because a window of opportunity was missed).
2. Potentially exploitable research results fail to make it across the so-called Valley of Death between research and innovation, e.g. because the opportunity is not recognised, because the required development investment cannot be secured, or because resources capable of achieving the innovation are not available.
3. Innovations projects do not achieve the intended impact, e.g. because product development fails, because the innovators did not really understand the requirement, or because a potentially successful product failed to catch on due poor marketing or just unfortunate market dynamics.

In the light of this analysis, the purpose of this study can be interpreted as to recommend ways of avoiding failures in these categories in the context of NIS-related research.

How research as such is done, is outside the scope of the study. Nevertheless, how the direction of research is influenced to make sure it will provide the raw material for successful innovation and hence significant impact is an important aspect of the study. Once funded collaborative research commences it is very difficult to change its strategic direction, although flexibility at a tactical level is possible. The research work programme, engages a call for proposals process and a selection process, which aims to influence market conditions toward economic growth and societal benefit. However, it is very difficult to anticipate the evolution of future demand. Thus, research projects need to address strategic issues that are likely to remain current over a long period and produce results that can potentially be exploited in many contexts using alternative technical platforms and product/service wraps. Strategic issues may need to be open-ended challenges rather than prescriptive goals, but should also allow the possibility of 'incremental exploitation' of results as research progresses. Identifying such topics is one main focus of this report.

Issues concerning the process of innovation and its coupling to research include:

- Adaptation of the direction of research during the life of projects as the market evolves;
- Effective use of application case studies, demonstrators and pilots to guide projects, validate results, and establish an effective two-way dialogue with 'innovators' and demand-side stakeholders;
- Activities that should form part of research projects in order to prepare the way for subsequent innovation;
- Incentives to reduce the financial risks of innovation
- Architectural frameworks, standards, infrastructure projects, as a means of encouraging a healthy and dynamic market.
- Education of researchers in business issues and the process of innovation. Encourage movement of people between research and innovation.

We also need to consider what distinguishes NIS from other domains when it comes to challenges and solutions regarding converting research results to social impact. The main characteristic feature of security that is not found in most other

problem domains is the existence of adversaries, with the adversary (usually) playing offence and the home team, defence. This has a number of implications:

- An attacker only has to find one exploitable weakness to succeed, whereas a defender must consider all possible attacks. This necessitates a holistic, 'systems approach' to security. There is always the danger that an innovation that improves security in one area will decrease security overall due to problems with compatibility with the rest of the security ecosystem. This will act as an inhibitor of innovation.
- Introduction of new technology and practices will often introduce new vulnerabilities and otherwise disrupt defences and create opportunities for an attacker. As we can expect the trend of accelerating innovation in business, society and leisure to continue, cybersecurity technology and practices must also innovate continuously. Even where established approaches to security remain valid, they will have to be transferred to new contexts and re-implemented, at least partly, using new technology bases. To minimise the need for re-implementation,

Security innovations should minimise dependence on implementation context. This could mean, for example, definition of an abstract pattern that can be applied in many contexts, or implementation as generic capabilities or services that can easily be coupled to an application platform via a thin integration layer.

- The iterated interaction between attack and defence drives an escalating arms race. Not only does this tend to accelerate the pace of innovation required in cybersecurity research, but also the co-evolution of attack and defence means that the direction of innovation is history-dependent and it is risky to predict future needs by extrapolating current trends.
- Measures taken to combat attackers tend also to impact legitimate stakeholders, thus security is often a question of balancing the rights of the individual against collective interests (e.g. privacy vs. surveillance, censorship vs. freedom of information). The optimal balance point is dictated by public opinion, and may swing violently and unpredictably in response to events (such as 9/11) and their media coverage. Consequently, basing security innovation on an absolute notion of values is likely to result in failure or rapid obsolescence.

The issue of the timescale mismatch between research and innovation raised earlier merits further discussion here. Innovation, as the term is currently used in business, is a process connecting an unsatisfied business opportunity or need with a novel tool, technique or idea, and usually resulting in a significant change to the way things are done (the word 'disruptive' is often used). As already noted, such demand is often difficult to forecast far ahead, and furthermore the window of opportunity for exploitation is likely to be limited. An innovator may identify an unsatisfied demand then search for new ways of satisfying it, or identify an emerging tool or technique and search for a recognised or latent demand. Either way, innovators must act rapidly to implement their innovations using the tools and techniques that can be applied within the time window.

This is in contrast to the traditional notion of development, which is more of a planned, technical process that takes as long as it takes. A significant obstacle to

innovation arises when effective and timely exploitation of a novel business idea depends on the availability of infrastructure, products or services that do not currently exist and would take too long to develop given the window of opportunity, and/or be too expensive to develop given the expected value of the specific opportunity. To help circumvent this obstacle:

The NIS research and innovation portfolio should include projects that are aimed at providing an innovation-friendly platform, i.e. a technological environment in which a range of novel applications, products and services can be brought to market or deployed, rather than at the applications, products and services themselves.

The difficulty in predicting future NIS requirements and the liability for those requirements to change rapidly, mean that it is more important that such a platform and the capabilities resident within it allow for a continuous and flexible evolution of services, rather than providing highly optimised support for a particular flavour of security service.

The need for a holistic, systems approach to security, and hence for a set of compatible and interoperating security capabilities mean that:

The NIS research and innovation portfolio should include projects that are aimed at defining and maintaining reference architectures, frameworks and interface standards, and encourage and co-ordinate the creation of ecosystems of compatible and interoperable products and services across a cluster of research and innovation projects. It is important that these architectures, frameworks and standards are defined in such a way as to promote competitive innovation, and are designed for evolution.

This will also encourage the establishment of a competitive European NIS market place, by lowering the barriers to entry to new players.

NIS research and innovation would be facilitated by the provision of shared experimental testbeds, avoiding wasteful duplication of effort and providing capabilities beyond the means of individual projects. These could include simulation of a range of application and threat scenarios. Cross-project experimental prototyping would be strongly encouraged. The testbed environments themselves could act as prototypes for innovation-friendly operational platforms.

1.4 Structure of the report

The body of the report is divided into four main sections as follows:

- Section 2 motivates the report by examining the potential financial return from investment in improved NIS and the products, services and technologies that enable it, and also at how well-placed the European NIS industry is to take advantage of the opportunities;

- Section 0 presents an overview of the NIS market; within the context of the overall ICT market and examines the challenges face by European players.
- Section 4 proposes a market demand-driven approach to identifying the key problems on which to focus future research investment. Consideration also has to be given factors such as: the likelihood and timescales of achieving success, the magnitude of the potential impact, and the prospects for take-up in the market place.
- The Process Definition & Innovation Models section takes an end-to-end look at research and innovation in cybersecurity, with a view to proposing new and/or improved process models that ensure that research remains focused on priority areas, and that results are translated efficiently into products and active use. In addition this section includes a number of case studies, which provide some understanding of innovation at SMEs and global organisations, with further examples of organisations that support innovation in the European economy.
- The main body of the document concludes with a Summary of Recommendations that reviews and combines the main insights revealed by the previous sections and documents these in concise form.
- There are also several appendices containing detail created and background information collected during the study.

2 Economic benefits of NIS research and innovation

The availability of new and improved NIS products and services will benefit the European economy in three main ways:

- By reducing the cost to European organisations and individuals arising from security breaches and related incidents;
- By addressing the risks (real and perceived) associated with new technologies and practices. Many people and organisations are reluctant to introduce potentially valuable innovations because of concerns over security. Enabling them to be used securely, allows the benefits to be realised.
- Increased revenue generated for European companies from new products and services, and the employment generated from growth in established businesses and creation of new companies.

The following sections detail these further.

2.1 Reducing the cost of security breaches

There are a wide variety of sources with respect to data breach statistics. One of the longest-running surveys is the Ponemon institute. In one of its recent reports², it presents evidence from a survey of 314 institutions in 10 countries (note: Ponemon Institute does not cover all of Europe, but includes U.S.). This study shows that in four European countries (DE, UK, FR, IT), an average number of breached record per institution of about 22.410). In the U.S. this number stood at 29.087. The average per capita costs of a data breach in U.S. dollars was in 2014 about \$201 in the U.S. and about \$169 on average across the four countries in Europe. To take one country example, reports such as the UK Government sponsored Cybersecurity Breaches survey³ run by PwC and Verizon data breach investigation report⁴ provide useful information on the scale of data breaches. In 2014, 81 per cent of large organisations and 60 per cent of small organisations in the UK had a security breach (2014 Cyber Breaches report⁵). Many studies have attempted to place a value on the cost of cyber-attacks to the national or global economy but, due to the lack of transparency as well as other statistical problems, estimates are sketchy and spread over a very wide range. (Oxford Economics report⁶). The 2014 Cyber Breaches report reports that the average cost of the worst breach suffered has gone up and is now £65,000 - £115,000 for small businesses and £600,000 - £1.15m for large organisations.

² <http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/>

³ <http://www.pwc.co.uk/audit-assurance/publications/2014-information-security-breaches-survey.jhtml>

⁴ <http://www.verizonenterprise.com/DBIR/>

⁵ <http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf>

⁶ <http://www.cpni.gov.uk/documents/publications/2014/oxford-economics-cyber-effects-uk-companies.pdf?epslanguage=en-gb>

There are a number of direct and indirect costs involved with data breaches, these are listed by the Ponemon institute. Direct costs involve computer forensics, victim identification, incidence response team, public outreach, notice documents and call centres. Other costs are consultancy services and legal services for defence, lost customer business and abnormal customer churn.

Organisations are often reluctant to report breaches because of the possible reputational damage that it can cause i.e. through loss of customer or investor confidence, it is reported⁷ that approximately 70% of organisations keep their worst security incidents under wraps.

2.2 Reducing the risk of innovation

The pace of innovation in business is accelerating. New technologies and business practices bring security challenges with them, and organisations are faced with a decision as to whether to delay implementation of an innovation that will yield business benefit (e.g. by reducing costs, streamlining business processes, improving customer experience, better understanding customer behaviour) until the security challenges are better understood and the means of mitigating them are available, or to proceed with the innovation and risk security breaches and their consequences.

This section discusses 3 emerging areas where this has been evident: Cloud computing, IoT and big data.

Cloud Computing is a loose collection of technologies and business models. There are many potential benefits that are attracting organisations to move their ICT infrastructure, business processes and/or applications to the Cloud, for example:

- Reduced capital costs;
- Increased agility (ability to scale resources dynamically);
- Reduced need for in-house technical expertise;
- Increased convenience and productivity (cloud storage and collaboration tools).

However, security concerns are often cited as the primary reason by organisations that have decided against, or are delaying, migration to the cloud. Such concerns include:

- Risks associated with shared tenancy (e.g. potential for competitors or malicious entities hosted on the same platform to gain access to sensitive resources);
- Dependence on the cloud service provider for availability and integrity of business-critical data and processes;
- Potential exposure to foreign legal jurisdictions and law enforcement and security agencies;
- Possible technical vulnerabilities associated with virtualisation, etc.

⁷Cyber Security Breaches Survey - <http://www.pwc.co.uk/audit-assurance/publications/2014-information-security-breaches-survey.jhtml>

Cloud security is gradually maturing, and more and more organisations are taking advantage of it, at least for less sensitive applications, but still concerns remain that are slowing take-up.

Another current trend of widening interest is the Internet of Things (IoT). This refers to the projected proliferation and variety of devices and appliances with embedded processing and networking capability. The ability to gather real-time information from such devices, process it and make decisions, then send out commands to implement those decisions raises opportunities for new services and efficiencies in many application domains, including power generation and distribution, traffic management, etc. However, there are security concerns⁸ that may either delay adoption if heeded, or cause damaging incidents if ignored, for example;

- Insecurity of individual devices – there have been reports recently highlighting the ease with which popular webcams can be compromised;
- Difficulty in updating/patching embedded software remotely;
- Complexity issues due to scale and interconnectivity networks that could make networks vulnerable to malicious or accidental disruption;
- Privacy issues due to the collection and aggregation of large amounts of data on various aspects of people's lives.

One of the central aspects of the ever increasing integration of digital technologies into everyday life is the fact that there is a related increase in the amount of data being produced, Big data as it is referred to brings with it tools and technologies that provide innovative opportunity and risk to organisations. These volumes of data are produced via a range of means including financial and consumer transactions, mobile telephony, and internet interactions to name but a few examples. With the adoption of each new digital technology comes a new stream of data, which is generated; new directions in technology such as the Internet of Things are set to increase this data flow even further. According to Google CEO Eric Schmidt while there were five exabytes of information created by the entire world from the dawn of civilization up to the year 2003, this amount is currently being produced every two days. Coupled with this is the fact that the cost of data storage has consistently decreased according to Moore's Law, meaning that there is the possibility of retaining this data and using it for other purposes. The value of data is evident in the fact that the most famous and valuable tech companies such as Facebook and Google are those which have data gathering and analysis at the core of their activities. The main innovation challenge of Big Data is that of realizing the utility of such vast data sets in a manner which is efficient, financially feasible and in keeping with legal and regulatory imperatives.

Big Data technologies are fast evolving and are at the forefront of technological innovation. The unique aspect of big data is that it involves very large data sets which when they are correctly gathered, stored and sufficiently cleaned can be used as a basis for analysing complex and diverse problems and uncovering non-causal relationships between factors. There are a range of spaces of innovation within the domain including infrastructure, analytics technologies, capabilities development and methodologies for handling and improving analytics results. Many

⁸ McAfee Labs Threats Report: November 2014:

<http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2014.pdf>

Big Data technologies are the result of combinations of other evolving technologies such as data storage, data handling, advanced mathematical models, automated analytics and data visualization. One current example of Big Data analytics usage is that which is used by financial institutions for the detection of credit card fraud. Prior to the usage of Big Data analytics fraud detection was a reactive process that was usually triggered by the customer reporting the card lost or stolen. By recording and analysing the aggregate credit card user patterns of all customers it becomes possible to identify deviations from these patterns on the fly. Such deviations are often indicative of cards being used fraudulently and so cards can be stopped which mitigates the risk of financial losses occurring. Big data analysis can also be used on social media outputs to conduct sentiment analysis, where user generated data can be harvested and interrogated to measure rates of response to given stimuli. This can be useful for gaining fine-grained analysis of responses to advertising or information campaigns and so can be used to measure their efficacy and to plan future campaigns.

Despite the potential power and utility of Big Data techniques and technologies there are some significant risks, which may hinder their use and adoption. These risks are mostly based around privacy and data protection, with concern growing amongst the general public as to the uses of their personal data in the wake of numerous reports of data breaches and the widely discussed problems relating to state surveillance. As well as this is the fact that many users are only now beginning to realize the value of their personal information and may begin to make claims for payment for its use. Such concerns can manifest themselves as innovation problems in a number of ways. Firstly if end users have privacy concerns which are not adequately addressed then they may be reluctant to use products which utilize big data methodologies; if products are not adopted and used then they will not make any money. A second way that privacy concerns could impinge on the sphere of big data innovation could happen where regulators and legal authorities act on these concerns and change laws or requirements which could prove restrictive for the development of new technologies or services.

Many of the potential risks associated with Big Data technologies can be assuaged using NIS technologies, standards, and practices. When implemented correctly, NIS technologies can perform the dual function of strategically supporting the benefits of Big Data while simultaneously countering any potential abuses that it may give rise to.

Supporting its benefits: NIS technologies will be supportive of Big Data in many different forms while reducing the Innovation risks that go along with them. The NIS Industry is using big Data methodologies intensively, which is one of the more mature Big Data market segments. For many years, NIS (IT Security) companies have been collecting data related to intrusions, vulnerabilities, malware, and other various incidents, in trying to identify the behaviour and activities of the hackers. This process is constantly being put under pressure due to the continued finding of new vulnerabilities and potential hacks into systems, networks and applications. This innovative nature of the hackers can be fought, by for instance discovering anomalies in operational systems. Anomaly detection uses big data technologies and advanced data analytics. Reducing innovation risk can be achieved by applying some of the proven techniques and mathematical models into other domains.

Countering abuse: policies in handling confidential information (and data) should fundamentally not be any different from any other types of data. This includes putting NIS technologies in place preventing access to personal data, or prevention of data leaking from big data stores. NIS technologies can also support encryption, anonymisation and de-personalisation of personal data. NIS expertise can help to identify instances where technologies used for personal data obfuscation, might even unintentionally identify a person because of their unique attributes.

2.3 Growing the European NIS product and services sector

The following sections give some context for the European NIS market in relation to the size of the market in economic and forecasting terms, size and growth by regional and product type categories. Some strengths and weaknesses of the European sector are identified with opportunities and threats explored.

2.3.1 How big is the global NIS market?

Different analyst sources define the NIS domain with varying scope, so depending on such scope these market size and growth estimates can vary considerably. Factors influencing this variation include the great amount of product and solution diversity within NIS, as well as the fact that many NIS solutions are increasingly embedded in wider ICT systems, making the value of the individual security and privacy elements more difficult to estimate. Table 1 below highlights a range of existing estimates⁹, with summary details of source references used highlighted in Table 2. Consensus estimates include:

- Globally the overall NIS market size is estimated to range from €46.9 - €76.3bn (or US \$58.8bn to \$95.6bn) depending on market definition and specific study scope. A narrower scope estimate of NIS related services by Pierre Audoin Consultants estimates the market for NIS “IT Services and Software” at €31.5bn (\$39.4bn) per annum at present (#5 in Table 1 and Table 2).
- Estimated NIS compound annual growth rates (CAGR) over the next five to seven years range from 8% to 13.4% per annum depending on study scope.
- By the end of this decade (2019/2020), it is estimated that the NIS market will be worth somewhere in the region of €115.8 - €123.7bn (or \$145-155bn) per annum.

⁹ Throughout this and other sections, currency amounts used are those used in the relevant original sources cited to ensure as much consistency with original analysis as possible. Where multiple currencies are stated for a single statistic (mostly Euro to US dollar conversions), the official rate at 31st October 2014 is used (€1 = \$1.252 USD, based on www.xe.com)

Source (#)	Market Size (Present and Future Estimates)	Future CAGR estimates	Defined Market Scope
[#1] Markets and Markets, April 2014 ¹⁰	NIS Global: USD\$95.6bn in 2014, estimated to grow to \$155.74 bn by 2019	Global CAGR of 10.3% between 2014-2019	Scope includes segment breakouts by security type (network, endpoint, application, content, wireless, cloud) and thirteen explicit solution type categories.
[#2] IDC/McAfee, Centre for Strategic and International Studies, June 2014 ¹¹	Global NIS addressable market \$58.2bn in 2013, up from \$53.6bn in 2012 Security "Product" portion worth \$32.1bn in 2013, up from \$29.9bn in 2012	8.7% growth between 2012 and 2013 NIS Product market portion running at 14.3% growth p.a. between 2012 and 2014	Bottom-up estimate leveraging several IDC analyst resources, containing 17 NIS product/service sub- segments plus estimate of other niche categories
[#3] Frost and Sullivan, February 2014 ¹²	NIS global market in 2014 worth estimated €62.4bn (~USD\$80bn) , increasing to €111.2bn (~USD\$144bn) by 2020	Global CAGR of 13.4% estimated between 2014 and 2020	Major cybersecurity applications analysed include network security, data security, end-point security, and ID and access control.
[#4] Gartner, August 2014 ¹³	Global Information Security Spending estimated at \$71.1bn in 2014, up 8% from 2013. Estimated to reach \$76.9bn in 2015.	8% CAGR estimated between 2013 and 2015	Definition of scope not entirely clear from press release
[#5] Pierre Audoin Consultants 2014 [18]	Security IT Services and Software Market estimated at €31.5bn (\$39.4bn) per annum in 2013	8.5% CAGR for segment expected between 2013 and 2017	Narrower in scope than #1 to #4 above, focus on NIS Services rather than hardware security appliances aspect so reduced estimate expected.

Table 1: Various global NIS market size and CAGR estimates from public sources

¹⁰ <http://www.researchandmarkets.com/reports/2820909/cyber-security-market-global-advancements#pos-10>

¹¹ <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf>

¹² <https://www.marketresearch.com/Frost-Sullivan-v383/Global-Cyber-Security-Assessment-8057049/>

¹³ <http://betanews.com/2014/08/22/information-security-spending-to-grow-8-percent-in-2014/>

Ref	Title	Reference
#1	<i>"Cybersecurity Market - Global Advancements, Forecasts & Analysis (2014-2019)"</i> Published: April 2014, Markets and Markets	http://www.researchandmarkets.com/reports/2820909/cyber-security-market-global-advancements#pos-10
#2	<i>"Net Losses: Estimating the Global Cost of Cybercrime"</i> Published: April 2014 Publisher: McAfee, Centre for Strategic and International Studies	http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
#3	<i>"Global Cybersecurity Market Assessment"</i> Published: February 17 th 2014 Publisher: Frost and Sullivan	https://www.marketresearch.com/Frost-Sullivan-v383/Global-Cyber-Security-Assessment-8057049/
#4	Gartner press release, Lawrence Pingree (Gartner Research Director) Published: August 2014	http://betanews.com/2014/08/22/information-security-spending-to-grow-8-percent-in-2014/
#5	<i>"Show Me the Money! Evaluating Market Opportunities in Cybersecurity"</i> Published: 2014 Publisher: Pierre Audoin Consultants	http://www.slideshare.net/nicolasbeyer/140326-pac-webinarcybersecurity

Table 2: NIS Market Size Resources – Source Details

2.3.2 NIS Market Size and Growth By Region

Based on statistics inferred from available Market and Markets data (Source #1 in Table 1 and Table 2) Table 3 summarises the present and estimated future breakdown of the NIS market by region (USD\$, billions per annum).

	2013 (USD, \$bn)	2014 (USD, \$bn)	2015 (USD, \$bn)	2016 (USD, \$bn)	2017 (USD, \$bn)	2018 (USD, \$bn)	2019 (USD, \$bn)	CAGR 2013-19	Global market share (2014)
North America	37.4	41.2	44.7	48.5	52.6	57.1	61.9	8.5%	43.1%
Europe	23.2	25.0	26.9	28.8	30.9	33.1	35.5	7.2%	26.2%
Asia Pacific	14.8	17.0	19.4	22.2	25.3	28.9	33.0	14.1%	17.8%
Middle East/Africa	6.2	7.1	8.0	9.1	10.4	11.8	13.4	13.7%	7.4%
Latin America	4.5	5.3	6.2	7.3	8.6	10.1	11.9	17.6%	5.5%
GLOBAL (TOTAL)	86.1	95.6	105.4	116.2	128.1	141.3	155.7	10.3%	100.0%

Table 3: NIS market size and growth by region, 2013-2019 (source estimates inferred from publicly available Market and Markets data, #1 in Table 2 above)

Global Regions: North America represents the largest market segment at present, valued in 2014 at an estimated \$41.2bn, with expected growth to \$61.9bn by 2019, an annual growth rate of 8.5%. Globally the North American segment forms just over 43% of global revenues at present. The combined European market is the second largest NIS region, worth approximately \$25bn in 2014, or 26.2% in global revenues. The growth rate in Europe is expected to be slightly less than that in the US, at 7.2% between 2014 and 2019, leaving a market size of \$35.5bn by that time. Asia Pacific is the next largest region at \$17bn per annum in 2014, but is expected to experience faster market growth than North America or Europe over the coming years, with 14.1% growth estimated between now and 2019, leaving a regional market of \$33bn, by then only marginally less than the future estimated European

market, and accounting for over one-fifth of global NIS revenues (21.2%). Other emerging regions are also expected to experience similarly high double digit growth - 13.7% growth in the Middle East and Africa segment, and 17.6% growth in Latin America.

Europe: Table 4 contains further breakdown of key countries within the European NIS market, with the UK, Germany and France forming the biggest market sub-segments within Europe, presently valued at \$4.4bn, \$4.0bn and \$3.3bn per annum respectively, and accounting for just under half of all European revenues at present (46%). All three countries are estimated to achieve growth rates of between 7-8% between now and 2019.

	2013 (USD, \$bn)	2014 (USD, \$bn)	2015 (USD, \$bn)	2016 (USD, \$bn)	2017 (USD, \$bn)	2018 (USD, \$bn)	2019 (USD, \$bn)	CAGR 2013-19	European market share (2014)
UK	4.1	4.4	4.8	5.1	5.5	5.9	6.3	7.2%	17.7%
Germany	3.7	4.0	4.3	4.6	5.0	5.4	5.8	7.7%	16.0%
France	3.0	3.3	3.5	3.8	4.1	4.4	4.7	7.7%	13.1%
Russia	1.8	2.0	2.1	2.3	2.5	2.7	2.9	8.0%	7.8%
All others	10.5	11.4	12.1	13.0	13.9	14.8	15.8	7.1%	45.4%
EUROPE (TOTAL)	23.2	25.0	26.9	28.8	30.9	33.1	35.5	7.4%	100.0%

Table 4: Key European Countries NIS Market Size and Growth, 2013-2019 (source estimates inferred from publicly available Market and Markets data, #1 in Table 2 above)

Other Countries: Other selected countries of note are highlighted in Table 5. Within the largest North American market segment the US market alone will account for \$33.7bn in NIS spending in 2014, over one-third of the global market (35.2%). Other key emerging regions such as Brazil, India, Saudi Arabia and UAE are each significant billion dollar plus markets in their own right, with each expected to experienced strong double-digit growth for the remainder of the decade. The NIS market in Japan is now worth \$4.8bn, and is estimated to grow to a \$10bn plus market by the end of the decade.

	2013 (USD, \$bn)	2014 (USD, \$bn)	2015 (USD, \$bn)	2016 (USD, \$bn)	2017 (USD, \$bn)	2018 (USD, \$bn)	2019 (USD, \$bn)	CAGR 2013-19	Global market share (2014)
USA	30.9	33.7	36.7	40.0	43.6	47.5	51.8	9.0%	35.2%
Japan	4.1	4.8	5.6	6.5	7.5	8.8	10.2	16.2%	5.0%
Brazil	2.6	3.1	3.7	4.4	5.2	6.1	7.3	18.7%	3.2%
UAE	2.5	2.8	3.3	3.7	4.3	5.0	5.7	14.9%	3.0%
Saudi Arabia	1.5	1.7	2.0	2.3	2.6	3.0	3.5	15.0%	1.8%
Australia	1.4	1.5	1.8	2.0	2.3	2.6	3.0	14.3%	1.6%
India	1.0	1.2	1.3	1.5	1.7	1.9	2.1	13.2%	1.2%
EUROPE (TOTAL)	23.2	25.0	26.9	28.8	30.9	33.1	35.5	7.4%	26.2%
All Others	18.9	21.7	24.2	27.0	30.0	33.2	36.6	11.6%	22.7%
GLOBAL (TOTAL)	86.12	95.6	105.4	116.2	128.1	141.3	155.74	10.3%	100.0%

Table 5: Selected Countries NIS Market Size and Growth, 2013-2019 (source estimates inferred from publicly available Market and Markets data, #1 in Table 2 above)

2.3.3 Market Size and Growth By NIS Product/Solution Categories

Much variation exists in how the NIS market can be decomposed into product/solution categories, and various analyst sources adopt different

approaches. A combined analysis of IDC report sources covered in a recent McAfee commissioned report [MCA14] (Source #2 in Table 1 and Table 2) indicates market sizes for several NIS product/solution sub-categories, as summarised in Table 6 below. While the overall market size estimate is more conservative than other assessed sources it provides a good indication of the relative size of different sub-segments and current growth rates.

Largest segments under this analysis include (Security) Integration Services (\$8.5bn in 2013), Firewalls (\$5.8bn), Consumer Security Products (e.g. Anti-Virus) (\$4.9bn), and Identity and Access Management (IAM) (4.9bn). Segments with the highest double digit growth rates include Forensics (21% year on year), Security Information and Event Management (11.2%), Vulnerability Assessment (10%) and IAM (10%). The increasing fragmentation and diversity of available NIS technologies is reflected in the “Other” Categories segment where a high growth rate of 14.2% exists.

	2012 (USD, \$bn)	2013 (USD, \$bn)	Share of PACs market (2013)	YOY growth (%)
Integration Services	8.1	8.5	14.6%	5.2%
Firewalls (General + Next Gen)	5.4	5.8	9.9%	8.2%
Consumer Security Products	4.6	4.9	8.4%	6.0%
Identity and Access Management (IAM)	4.4	4.9	8.3%	10.0%
Consulting Services	4.4	4.7	8.1%	7.5%
Corporate Endpoint	3.4	3.7	6.3%	7.1%
Email Gateway	2.4	2.6	4.5%	7.2%
Web Filtering	2.0	2.1	3.6%	6.6%
Intrusion Prevention Systems	1.9	1.9	3.3%	2.5%
Security Information and Event Management	1.4	1.6	2.7%	11.2%
Vulnerability Assessment	0.9	1.0	1.7%	10.0%
Policy and Compliance Solutions	0.9	1.0	1.7%	9.9%
VPN	0.7	0.7	1.3%	2.9%
Proactive Endpoint Risk Management	0.5	0.5	0.9%	5.0%
Forensics	0.3	0.4	0.6%	21.0%
Security Device Systems Management	0.2	0.2	0.3%	-7.3%
Other Categories (2012, 2013)	12.1	13.8	23.7%	14.2%
	53.6	58.3	100.0%	8.7%

Table 6: Current market sizes by NIS solution sub-segments (adapted from McAfee Report, Source #2 in Table 2 above)

While the paragraphs above indicate a significant growth opportunity for European industry, it must be acknowledged that this opportunity is widely recognised and the NIS products and services sector is already very competitive. Not only are there established specialist NIS vendors, but also major multinational corporations from adjacent sectors such as IT, Telecommunications and Defence who are expanding their NIS businesses rapidly through both internal growth and acquisition and mergers. For example, IBM has acquired 12 security companies in the past decade, and has invested more than \$2 billion into security research, garnering more than 3,000 patents in this area.

NIS research needs to consider market conditions in relation to market entry, volatility and maturity. Technical research can facilitate a multi-disciplinary approach to maximise the impact of NIS research. The chasm between research and technology transfer is surmountable and product bundling particularly targeting the SME segment has the potential for NIS innovators to penetrate the market efficiently. Strategic alliances with technology and service providers can facilitate products and services to be targeted toward individual users and SME's.

2.3.4 EU NIS market strengths and weaknesses

The previous sections illustrate Europe's current share of the Global NIS market and some forecasts for the future. This section presents some of the strengths Europe has built up in this area and weaknesses that Europe might acknowledge in this sector. Further work is ongoing through existing projects and recommended in the SRA in this area to detail the opportunities and threats in this domain.

Strengths

- Trust in the security and privacy of EU-based solutions and products
- Increased need for specific security solutions for EU Industries (IoT, telematics, industrial internet)
- Tailored solutions for EU requirements
- Privacy regulation fostering trust; legal and regulatory framework supporting free and open cyberspace.
- Proven research capability in our 3rd level education systems
- Strong regional knowledge expertise amongst local players in their captive markets –e.g. “made in Germany” principle. Often gives such players a sustainable competitive advantage locally
- Regional leadership in demand for better privacy technologies in step with EU leadership in privacy legislation and enforcement (e.g. EU Data protection directive, right to be forgotten, Google ruling etc.) and leadership in developing appropriate solutions
- New private cybersecurity-specific funds emerging in the region (e.g. C5 Capital)
- Valuations of European companies in global investment marketplace more attractive versus other regions (e.g. US)
- Notable acquisitions of key European companies in recent times (e.g. Stonesoft, Alaric, Contextis, Arkoon), as well as notable funding investments (e.g. Alienvault)
- Improved publically funded instruments – e.g. SME H2020 instrument, similar to SBIR instrument in the US
- Large number of NIS clusters regions developing and growing throughout Europe (CSIT, Hague Security Delta, LSEC, Teletrust, Malvern + UK Cybersecurity Forum).

Weaknesses

- Market fragmentation
- Limited access to venture capital
- Limited collaboration culture between security companies
- Niche players without critical mass; lack of mass-market presence
- Limited export capability in SMEs
- Less attractive Venture Capital ecosystem in Europe versus other leading NIS regions (US, Israel) – particularly for post Series A funding rounds
- Exit strategies of European players often involves early acquisition by US players who are attracted by the low valuations of European players, meaning that impact of players on European marketplace and industry is less well felt
- Lack of instruments supporting NIS SMEs in funding initial idea generation and customer engagement
- Stronger and more advanced innovation ecosystems exist around the defence/military sectors in other regions, leading to more advanced R&D and better innovation outcomes in NIS (US and Israel in particular)
- Large proportion of NIS products/solutions used throughout Europe are imported from manufacturers in other regions (US in particular), greater self-sufficiency desirable

The IPACSO project www.ipacso.eu deliverable¹⁴ Market and Regulatory Environment and Industry Analysis report further details the strengths and weaknesses of the European NIS industry and provides, for example, PESTLE Analysis of Key PACs Domain Trends (section 4) and a global competitor view (section 6). Its recommendations are specific to the European NIS industry.

¹⁴ <http://ipacso.eu/downloads/category/9-ipacso-project-public-deliverables.html>

3 Market and Industry overview

3.1 Introduction

To contextualise the business cases we provide a market and industry overview so that one can visualise how the selected business cases fit into the overall market environment. The market analysis plays an important role in validating potential innovation paths however; it is necessary to be cognisant that a full market analysis is not within the scope of this deliverable. It is helpful to identify a common language to position this study. Thus, we need to agree on different types of stakeholders (individuals, organisation, institutions of various types) and product/services value chains as well as innovation value chains in the cybersecurity market. There are some established markets for security products and the overall objective of this deliverable is to highlight possible market demands in the early stages of emergence or not yet identified. At this stage, only a very generic supply chain model for security products and services in the cybersecurity domain can be provided. However, this model allows different stakeholders to identify where they are in the supply chain and analyse potential vertical problems.

Markets can be analysed by using a horizontal perspective, i.e., identification of firms that compete with one another while being located at the same stage of the supply chain. This perspective is typically used in competition analyses conducted by authorities or researchers.

The following market definition is proposed: “The cyber-security market is a physical or virtual place, where demand and supply for cyber-security products and services meet.”¹⁵ In order to be a relevant player in the market, a company needs to offer at least one, if not a portfolio of cyber-security products and services. Ideally, a player generates the larger share of revenues through the sale of these products and services.

Firms, in turn, often segment markets by identifying different consumer/end-user groups. This is a method used in marketing. It allows the tailoring of products or services to these segments. Segmentation, however, also facilitates a better understanding of markets for other stakeholders such as policy-makers. The cybersecurity market is not particularly mature and thus segmentation for this domain would not be considered stable and can differ in some reports.

Markets can also be analysed in a vertical perspective, i.e. by identifying the stakeholders at different levels of the supply chain. A supply chain connects input (such as raw materials), the different production stages and the output (product and/or service) in a chain-like model. Output produced in one industry, for example by cyber-security firms, can constitute the input into another industry such as banking and finance. The identification of such interrelationships is important from an overall macro-economic perspective as information technologies are

¹⁵ Jentzsch, N. (2014a). Horizontal and Vertical Analysis of Privacy and Cyber-Security Markets, IPACSO Deliverable D44.2 (A), *unpublished manuscript*, p. 12

increasingly seen as economic enablers. Furthermore, the increased integration of supply chains has an impact on the vulnerability of players and resilience of the overall system.

The complexity of the interrelationships in networks as well as the complexity and immateriality of many of the products and services provided by cyber-security and privacy firms, the lack of data and reporting requirements, as well as the existence of confidentiality requirements hamper the analysis of the market.

In order to analyse the market we consider stakeholder categories, supply chain roles and market segments. The stakeholders are the people or organisations that have requirements regarding the security of an ICT-based system (process or application). The supply chain roles are categories of person or organisation that contribute to the required security.

The stakeholder categories proposed for the purposes of this study are:

- End user (of the ICT-based system, may be e.g. an employee, member, or customer of the owner/operator)
- Owner/operator (of the ICT-based system)
- Regulator (a government agency or other third party with an interest in protecting the other stakeholder or the wider community)
- Dependent third party (who may suffer if the security of the system is compromised e.g. the subject of personal/sensitive information held in the system).

Section 4.1 below describes specific stakeholders in relation to demand-side stakeholders and innovation stakeholders in detail.

The proposed supply chain categories are:

- Security Technology provider
- Infrastructure provider
- Systems integrator
- Service provider / retailer
- Security operations

There are numerous ways to segment the cyber-security market, for example according to generic type of product or service (hardware, software and services, see below). In fact this type of classification is the most common one in research studies on the topic. In business, firms often use segmentation according to industries (also called 'verticals') such as banking, health and energy.

It is possible that an organisation can be involved in more than one stakeholder category, supply chain category or market sector depending on their market offering and product line(s). The following sections give further detail on market segmentation, technology vendors and market growth predictions.

The cybersecurity technology service product market is challenging, an environment of compatible products and services is visionary. Indeed, each of the major players adopts their own cybersecurity policy and funding mechanisms. A review of the EU Cybersecurity policy performance is underway its results will increase our focus in this area.

3.2 Horizontal and vertical market analysis

As explained in the introductory section, **horizontal market analysis** allows for an overview of the industry as well as the competitive landscape. The most important classification used is hardware, software and services in order to identify the relevant players in these markets.

Of central importance is the definition of a relevant product or geographical market.¹⁶ A relevant market encompasses all products and/or services, which are regarded as substitutable by the consumer. At this stage, we cannot go into the details of market definition itself. It is sufficient to state at a general level that the horizontal perspective also allows the analysis of market structure, conduct and segments.

Market segmentation divides a market into segments that group products/consumers/distribution areas along common criteria. There are several different approaches on how to segment markets. The approach employed depends on the goal is to be achieved. For example, if statistical analysis of ICT industry importance is intended, the respective actor will use the hardware, software and services segmentation for association with international schemes such as the European industry classification system, NACE (Nomenclature statistique des activités économiques dans la Communauté Européenne). If better marketing of products is intended, the actor will possibly choose segmentation into different buyer organizations.

In the following, some examples of segmentations and their sources are listed.

It is possible to segment a market by:

- Generic type of product/service: Hardware, software, services¹⁷
- Buyer organization: Government (defence and intelligence), government (other than defence and intelligence), large enterprises (>250 employees), SMEs & consumers¹⁸
- Security solution: Infrastructure, systems, contents and governance¹⁸
- Basic technology: Authentication, authorization and access control, system integrity, cryptology¹⁹.
- By geographical market: North America, Latin America, Eastern Europe, Western Europe, Africa and Middle East and Asia Pacific.

Essentially, different types of segmentations can be combined, for example, the segmentation by generic type and geographical region.

In the FIRE research (TrustworthyICTonFire) market research was done with five vertical industry sectors: Energy, Healthcare, Finance, Government and ICT-

¹⁶ Commission notice on the [definition of relevant market](#) for the purposes of Community competition law [Official Journal C 372 of 9.12.1997]. See also:

http://europa.eu/legislation_summaries/competition/firms/l26073_en.htm

¹⁷ BMWI <http://www.bmw.de/DE/Themen/Digitale-Welt/sicherheit.did=360708.html>, INTECO (2009).

https://www.inteco.es/CERT/publications/Studies/Study_ICT_security_sector_Spain

¹⁸ PAC – Pierre Audoin Consultants (2013). Competitive analysis of the UK cybersecurity sector, Study, <https://www.pac-online.com/competitive-analysis-uk-cyber-security-sector>

¹⁹ State-of-the-art Secure ICT Landscape <https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/state-of-the-art-of-the-secure-ict-landscape/view>

Mobile. The FIRE project report²⁰ contains a summary of the user needs for Trustworthy ICT, expressed by their end users. The itemised 'topics' represent groupings of the user needs that represent larger potential user-derived research 'themes', which could be defined as cross-sector :

1. Establishing trustworthy relationships
2. Information privacy, assurance and cybersecurity
3. Addressing implications of trends in scale and complexity
4. Encouraging and supporting appropriate user behaviour
5. Proving fitness for purpose

It is important to note that segmentation methods that are not technology neutral will have to incorporate and exclude technologies over time, which makes inter-temporal comparisons more difficult. Moreover, segments ought to be clear enough to give some guidance on what entity belongs into what category. If definitional classification is not possible or only difficult to achieve the segmentation becomes fuzzy.

For the first iteration of this deliverable we have identified the following market segments.

- a) Identity and Security Services
- b) Trusted Service Infrastructure
- c) Secure Engineering (Tools and Methodologies)
- d) Security management solutions

Upon consultation with the wider NIS WG3 group of contributors we may decide to align these segments to our proposed business cases or we may decide to expand upon our suggested list.

Vertical analysis (or supply chain analysis) requires the identification of different stages of the production chain by connecting inputs to outputs. Supply chain analyses offer insights into the production process of cyber-security goods and services. In today's interconnected world, however, it is more appropriate to speak about supply networks (i.e. the interconnection of different supply chains).

The difficulty of clear identification of supply chain stages stems from the immateriality of the product/service provided ('security of information and information systems'), as well as the complex interrelations of players. Moreover, ICT security and privacy is an issue cutting across sectors, industries and institutions. ICT security production may involve 'self-standing products/services' (such as a personal data vault),²¹ but can also be an integrated feature of a product or service (such as a more privacy-friendly social network).

At the most generic level, the following stages can be identified, presented in Figure 2.

²⁰ Industry Sector Research Needs, Trustworthy ICT Research in Europe for ICT Security Industry, ICT Security Users and Researchers, FIRE 2014. <http://www.f-i-r-e.eu>

²¹ Information goods often require an infrastructure, such as the Internet. What is meant here is that a personal data vault is an identifiable separate product/service.

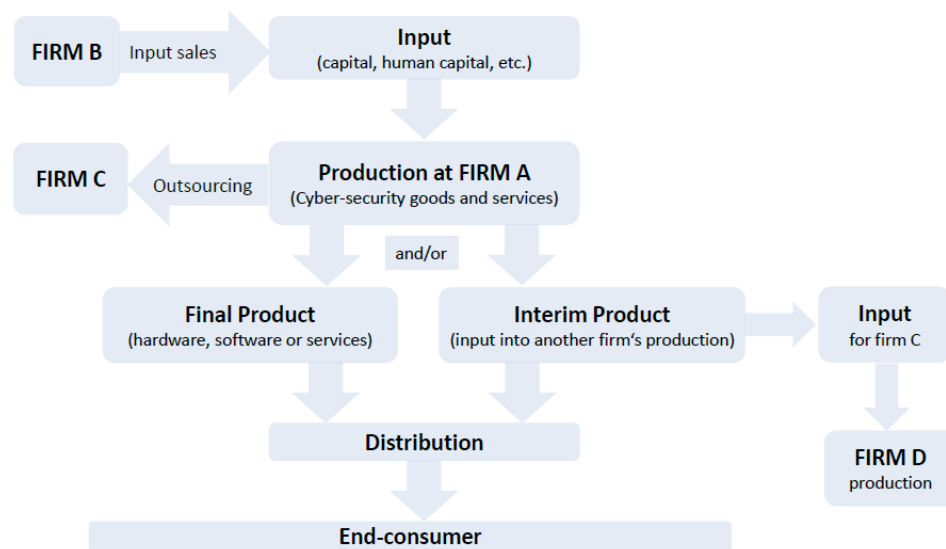


Figure 2: Cybersecurity Supply Chain, Source: Jentzsch, N. (2014)

The input into cyber-security products and services relies on purchased inputs such as capital equipment (e.g. hardware) and human capital, including research and development. These 'raw materials' are processed into products and services that are intended to increase the level of information security for the end-user. At the production stage, a firm may outsource some of its activities.

The outputs are either final products (such as Anti-Virus software) or they are intermediate products that act as input into another industry's production (e.g. security solutions for banking and finance institutions).

In general, much more research must be devoted to the identification and analysis of horizontal as well as vertical features of markets for cybersecurity and privacy.

Horizontal mapping of markets allows for a comparison within European countries as well as an evidence-based analysis of weaknesses (e.g. lack of independent hardware producers).

The vertical mapping of supply chains allows for a more in-depth analysis of industrial relations as well as economic incentives of players to forward or backward integrate, for example. The impact of such relations is also unclear from a resilience perspective.

Moreover, additional insights will arise by combining the two types of analytical perspectives. The first steps to be conducted here are additional efforts put into definition of relevant markets for cyber-security and privacy as well as better analytical tools and a better information basis on vertical supply chains.

It is possible to segment the buyer market into four sub-segments: defence and intelligence, government (other than defence and intelligence), enterprises and SME & consumers. The least mature of these market segments is that of SME & consumers and so this represents a business opportunity that we recommend is further developed.

3.3 Global technology vendors

The competition in cybersecurity and privacy markets is characterized by some dominant international players that are often of an Anglo-American origin and numerous smaller players that are often specialized in specific segments such as cryptography. In addition, the competition may be characterized as innovation competition as there is often not only competition in the market for clients, but for the markets when new products are developed.

Global IT giants such as IBM and HP have reinitiated their security strategies. Services generalists such as CSC and CGI have security established in their IT infrastructure practices, as most projects include security, e.g. building a universal client, exchange platforms, infrastructure-as-a-service etc. CGI Group now ranks as one of the largest providers of cybersecurity services in the UK following its acquisition of Logica in 2012, which delivered systems integration and outsourcing engagements in secure environments such as central intelligence, defence and national policing agencies.

For example, manufacturers of supervisory control and data acquisition (SCADA) systems such as ABB and Siemens will increasingly need to be considered as part of the cybersecurity universe as they build greater security defences into their systems in the wake of the Stuxnet attack of 2010, which targeted industrial systems.

ENISA suggests that government-backed cyber pools may be needed and stresses the need for mandatory breach reporting. There is a danger of the market focusing on consequences instead of front line effects of cyber failings.

Upon further analysis the innovation case studies from BT, HP, SAP, ESPION, Technikon, Eng, ATOS and LSEC in this deliverable will contribute further to this section.

3.4 The European Solutions for Cybersecurity

To better understand the landscape, we conducted an initial SWOT analysis of the EU-based cybersecurity players citing the following reports.²² The European Union has been a leading player in the global cybersecurity market. This is a consequence of its strengths. This includes long-term focus on cybersecurity, trust in EU-based solutions, and global reach of the developed solutions. We recommend that a full SWOT analysis by experts in this field is conducted to complete the full picture.

²² Pierre Audoin Consultants: Competitive analysis of the UK cyber security sector for the Department for Business, Innovation and Skills, Version 1, July 29, 2013.

Der IT-Sicherheitsmarkt in Deutschland - Grundstein für eine makroökonomische Erfassung der Branche (engl. „the IT Security Market in Germany“), Bundesministerium für Wirtschaft und Technologie (BMWi), Berlin, August 2013

3.4.1 SWOT Analysis

Strengths <ul style="list-style-type: none"> • Innovative solutions that cover global needs. • Trust in the security and privacy of EU-based solutions and products • Tailored solutions that address specific EU requirements. • Privacy regulation fostering trust; legal and regulatory framework supporting free and open cyberspace. • Workforce mobility across Europe; educated workforce 	Weaknesses <ul style="list-style-type: none"> • Market fragmentation • Limited access to venture capital • Limited collaboration culture between security companies • Niche players without critical mass; lack of mass-market presence • Limited export capability in SMEs • Long cycles from innovative ideation to commercial products
Opportunities <ul style="list-style-type: none"> • Export opportunities due to good reputation of EU products. • Increased need for specific and tailored security solutions for EU Industries (IoT, telematics, industrial internet) in particular for SMEs • Increased regulation as market enabler (e.g. German regulation for critical infrastructures) • Local supply chain for services supporting SMEs. 	Threats <ul style="list-style-type: none"> • Free (AVG) or bundled (Microsoft Defender) supply of security products. • Lack of sufficient skilled personnel in the ICT Markets • Increased research funding and product development in emerging economies, at more favorable cost • Regulatory and certification requirements for indigenous products in emerging markets • Increasing regulatory burden in EU

3.4.2 Strengths

The EU IT Industry has a long-term history in innovative IT Security solutions that have usually also been marketed globally. This enabled the EU cybersecurity companies to establish trust globally. This includes security as well as privacy due to the comparatively strong privacy regulations and traditions in Europe.

Based on the needs of the EU market, the companies have designed and built a wide range of security technologies that address the specific needs of given markets. Examples are smartcards and security hardware for banking applications, antivirus and intrusion detection, as well as government security offerings.

Cybersecurity skills are in high demand; highly educated and mobile work force in Europe as well as the ability to attract the best technologists from outside of Europe is a clear strength.

3.4.3 Weaknesses

While the EU players are often leaders from a technology perspective, translating these technologies into profitable business opportunities is often inhibited by the weaknesses of the European ecosystem.

A first inhibitor is the fragmentation in many small markets that are served by niche players. Even if expansion into a global market is possible, these players lack the critical mass, knowledge of global markets, and finances to scale globally.

A second inhibitor is the limited supply of venture capital that renders growth of new ideas slow and risky for the founders. This in turn may lead to missed windows of opportunities due to slow growth.

Additional weaknesses include relatively low rate of startup emergence compared to other developed countries and relative long cycles from ideation to commercialization.

3.4.4 Opportunities

Due to recent events, the opportunities for cybersecurity solutions has been substantially expanded. While in the past, generic solutions aimed at securing a broad range of applications (“a firewall and antivirus is all you need”), most sectors now realized that they need tailored security services and solutions that address the specific risks of their industry (IoT, telematics, industrial internet). A specific opportunity is to design and offer automated and simple solution for the large SME sector in Europe.

Based on the good reputation of EU technology and companies, global export is simplified by the high level of trust in European technologies. This allows some companies to scale beyond the EU markets.

For the local markets, opportunities are created by potentially increased regulation (e.g., draft NIS directive and related regulations in Member States) that drives the need for cybersecurity solutions. A final opportunity is to service the SME market that is dominated by local business relationships.

3.4.5 Threats

For traditional security solutions (such as Antivirus), a consistent threat has been commoditization and the free inclusion in other products. Examples are free Antivirus products or bundling of security along with operating systems. This requires companies to continue to innovate and offer substantial value beyond these free offerings.

A second risk is the lack of skilled IT personnel. Already today, a shortage of experts can be observed and growth of the market will be inhibited unless sufficient numbers of experts are trained in cybersecurity.

Other risks include changing environment in emerging economies, increasing their competitive potential and decreasing export opportunities for the EU countries. Growing cost of compliance in Europe also represents a potential threat

3.5 Conclusion

In line with research in this area²³ the cybersecurity market today faces five major challenges:

²³ IPACSO EU funded project www.ipacso.eu deliverable D2.2 Market and regulatory environment and Industry analysis Report
CYSPA EU funded project www.cyspa.eu deliverable D3.4 – Uptake Innovation Models

- **Lack of market knowledge:** There is a lack of publicly accessible market knowledge in the form of standardized market definitions, statistical information, market monitoring and trend analysis.
- **Research into product transfer:** Europe has many outstanding research outcomes, yet they often fail to reach the market.
- **Awareness:** Existing cybersecurity products do not always reach the customer
- **Regulation:** Each country has specific regulation and legislation toward data and privacy this impacts the pan-European service and product offering.
- **Sensitivity for end-users:** Citizens of Europe are particularly sensitive to cybersecurity. The impact the digital environment has on personal lives, accessibility and vulnerabilities is unique and thus the risk associated is difficult to measure and mitigate against.

4 An approach to prioritising research topics

This section develops a demand-side requirements-driven approach to identifying the key problems on which to focus future research investment in order to maximise the potential impact of available funding. The idea is that targeting challenges associated with high priority, unmet requirements will result in novel techniques and technologies that enable innovative and marketable products and services. Recommendation of research topics is the responsibility of the SRA activity, and will not try to usurp that. However, we hope that the ideas presented here will influence the process of constructing the SRA and the direction of future NIS Research Roadmapping activities.

The primary selection criterion is an estimate of the potential impact of expected research results, which will depend as much on how widely the results could be used as on the impact of an individual application. Consideration also has to be given to factors such as: the likelihood and timescales of achieving success, the magnitude of the potential impact, and the prospects for take-up in the market place. It will often not be possible to perform an objective quantitative analysis, but analysis based on subjective, qualitative judgement will still be useful.

The approach proposed is as follows

1. Identify significant stakeholder roles. Describe security concerns/requirements from the points of view of each of these stakeholders, including the impact of not meeting the requirements.
2. Define an approach to cost-benefit analysis of research topics to be used in step 5.
3. Identify and describe in outline a number of scenario-based case studies in which security plays a significant role, and which collectively are representative of the NIS domain. At least some of these should exemplify emerging / novel business models. Identify steps in which security is a critical factor and describe the outstanding challenges.
4. Select a sub-set of these scenarios and perform a more detailed analysis.
5. Derive a set of candidate goal-oriented research topics for evaluation from the outstanding challenges identified in the scenario-based case studies, and from additional sources (research agendas, active research areas as indicated by publications, etc.). Evaluate these qualitatively from the points of view of: required investment and resources, potential impact (referencing the scenario-based case studies), likelihood/timescales of achieving success, and route to market, dependencies on each other and other factors, etc.
6. Based on the above analysis, propose a recommended 'portfolio' of research investment opportunities.

As part of this study we have worked through steps one and two, and several outline case studies have been drafted to gain experience of applying the methodology.

4.1 Stakeholders and requirements

We examine requirements from the points of view of two main types of stakeholder in the NIS Research and Innovation process:

- Demand-side stakeholders: these are participants or interested parties in the scenarios in which the eventual results would be used, whose needs influence the requirement for security or how it is provided or overseen. The extent to which their needs are met by existing offerings dictates the demand for innovation;
- Innovation/supply-side stakeholders: these are participants in the value chain required to bring products and services 'to market' to fulfil unmet demand.

4.1.1 Demand-side stakeholders

4.1.1.1 *Classification of stakeholders*

Clearly, innovation cannot succeed unless the product of the innovation process meets some previously unfulfilled requirement, or significantly improves on an existing solution. Often, demand is only created when a novel product appears on the market, and sometimes disruptive changes can be brought about when end-users find an application of a product that is different from that intended by its makers. Nevertheless, the requirement must exist for the product to be successful, even though it may be latent and waiting to be discovered.

It is important, therefore, to be guided by an understanding of who the demand-side stakeholders are, what facets of security are important to them, and which of these are likely to remain or become problematic in the absence of a significant change in the way security is provided. We propose the following as a working set of categories that capture the essentially-distinct demand-side perspectives on the security of a system:

- Owner/operators of the ICT-based systems or processes being considered. These are the primary stakeholders, who would be the customers for the innovation, and in most cases would be responsible for paying for its introduction and operation. For an owner/operator to decide to implement an innovation, the potential benefits (reduced risk exposure, losses due to security breaches, cost of security controls, etc.) must comfortably outweigh the expense and disruption involved. A responsible owner/operator will establish a security management system that sets, implements, operates, and monitors the effectiveness of policies designed to maintain a security risk exposure in line with the organisation's risk appetite.
- End user: person using the ICT-based system or participating in the process. The end-user may be e.g. an employee, member, or customer of the owner/operator. End-users do not (usually) decide on or pay for implementation of a security innovation or gain from security improvements. However, their acceptance of the innovation plays a key role in its success. Usability is often a key factor: if a security innovation makes it more difficult for employees to do their jobs, they will tend to ignore or circumvent it. This may result in an expensive new system remaining largely unused, and

security may even be made worse. It is useful to distinguish between end-users playing roles in application/business processes, whose security requirements will mainly be non-functional, and those involved directly in security/control processes who will also have functional security requirements.

- Regulator (a government agency or other third party with an interest in protecting the other stakeholders or the wider community). A rational owner/operator will invest in security controls that protect its own interests provided the benefit out-weighs the cost. However, a formal or informal oversight institution may be required to protect the interests of other stakeholders or ensure that societal goals are met. Typically, the regulator will prescribe some standard of behaviour to be followed by owner/operators (and other stakeholders) in some domain. This standard will need to be monitored/audited to measure compliance, and some appropriate sanction imposed in the event of non-compliance. Regulations can encourage innovation (e.g. by creating a more open and dynamic market, or by mandating change), but there is also the danger that innovation may be stifled by regulations that effectively enshrine the *status quo*, make change too slow or risky, or create barriers to entry into the market. It is also possible that regulators with conflicting remits may issue contradictory requirements, resulting in uncertainty.
- Dependent third party (who may suffer if the security of the system is compromised e.g. the subject of personal/sensitive information held in the system).

Consider, for example, a health care information systems context; the stakeholders might be:

- Owner/operator: the health care provider. Its primary concern is to ensure that accurate and appropriately-detailed patient information is available to health care staff when and where they need it. It may also have relevant secondary concerns such as providing information for research studies, inventory control, resourcing, billing etc. Major security threats include:
 - Corruption of information leading to inappropriate treatment, endangering patients' health, and even lives, and exposing the provider to legal action and loss of reputation. If the corruption is detected prior to treatment being given; then the consequences are similar to system failure.
 - System failures/poor performance means that information is not available where and when it is needed. Consequences can include failure to provide timely treatment (with impact on patient health) and waste of time and resources.
 - Breach of regulations / industry standards could result in fines, loss of approved status / enforced re-organisation, and loss of reputation.
 - Fraud and theft of drugs.
- End-users:
 - Healthcare professionals, administrators, etc. will mainly see security measures as potential obstacles to them doing their jobs. It is, of course, vital that security measures should never endanger the life or health of patients.

- Security professionals: responsible for deploying and operating the controls that implement the health care provider's security policies.
- Regulators:
 - Regional and national bodies responsible for ensuring appropriate levels of healthcare are available to citizens.
 - Bodies responsible for ensuring personal data is protected
- Dependent third parties:
 - Patients/citizens are concerned about receiving appropriate and timely healthcare at affordable cost, and also that their personal information is not disclosed.

4.1.1.2 *Differences between market sector*

If we look at the market sectors identified in the report, “*Competitive Analysis of The UK Cybersecurity Sector*”, which was compiled by Pierre Audoin for the UK Department of Business, Innovation and Skills (BIS, see section A.1), i.e.:

- Defence and intelligence
- Government, other than Defence & Intelligence
- Enterprises
- SMEs (Small and Medium-sized Enterprises) and consumers

Representatives of the stakeholder categories can be found in each case, with both similarities and differences across sectors. The Government and Enterprise sectors are generally similar, except that enterprises primarily serve the financial interests of their owners or shareholders, while government organisations serve societal interests as expressed in government policy. They are typically large organisations with a full range of stakeholders generally as described above. They have substantial, though bounded, financial and human resources, and can be expected to take charge of their own NIS e.g. via a risk-based security management system, though they may elect to outsource some security functions to professional and managed service providers. Relevant types and impact levels of risk will vary considerably, but will generally be mid-ranking.

Defence and intelligence organisations will have more specialised and extreme requirements. They will often be dealing with information of extreme sensitivity, and the impact of security failures could be very severe – at worst risking national survival. Although still subject to the rule of law, additional (including offensive) options available to them. Although still finite, financial resources and numbers and security skill level of human resources are likely to be large. Furthermore, essentially limitless funding could be made available by governments in times of crisis. They are less likely to outsource security functions, but may do so to approved contractors with specialist capabilities on occasion.

SMEs and consumers are at the opposite extreme. In reality, they are distinct markets, but are often lumped together because they have some shared characteristics (notably very limited security skills and financial resources). The

term SME covers a wide range of entities in terms of size²⁴, nature of business and security needs. Like larger enterprises, they really require tailored security solutions; however, they cannot afford to pay for them. Consequently, they are a difficult market for vendors to serve, and they end up being offered off the peg products and services with substantial commonality with consumer offerings. Similarly, the size of SMEs in personnel terms means that at best a small number of staff will be tasked with responsibility for security, and they will most likely cover other roles as well. They are unlikely to attract staff with a high level of security expertise, aptitude and interest, not only because of salary, but also technical interest and career progression. Providing existing staff with security training will give them marketable skills and so they will be difficult to retain. Although in absolute terms the impact of an SME security breach will be low, a serious breach could still be fatal to the company. Furthermore, the aggregated impact of breaches across the SME sector could well be economically significant to member states and the European Union as a whole.

The situation with consumers is even more extreme. Arguably, all the stakeholder roles still apply, but typically the owner/operator and end-user will be the same person – the consumer. The consumer may be aware of security issues, unless he/she (or a relative or member of the household) is coincidentally a hobbyist or a professional, technical and security skills are likely to be minimal. Furthermore he/she will be unwilling to pay more than a modest premium for ‘secure’ products and services. Ideally security should be free, built-in, invisible unless user-input or action is required, very easy to use when it is, and have minimal effect on other user activities and pursuits.

4.1.1.3 Persistent trends

The stakeholder model and discussion of requirements given above is largely independent of era; it is valid now and is likely to remain so in 2025. It is widely acknowledged that NIS is currently in crisis, with improvements required in all areas. Traditional security models and controls are proving insufficient in the face of today’s threats and trends in technology and usage, yet the way forward is far from clear. The following is an excerpt from an article from McKinsey&Co²⁵:

Why isn’t more being done to protect critical information assets? Senior executives understand that the global economy is still not sufficiently protected against cyberattacks, despite years of effort and annual spending of tens of billions of dollars. They understand that risk alone undermines trust and confidence in the digital economy, reducing its potential value by as much as \$3 trillion by 2020. They understand most institutions have technology- and compliance-centric cybersecurity models that don’t scale, limit innovation, and

²⁴ In the BIS report, SMEs have 250 employees or less, but other sources may use different definitions.

²⁵ Tucker Bailey, James Kaplan, and Chris Rezek, ‘Why senior leaders are the front line against cyberattacks’, McKinsey&Company, June 2014, http://www.mckinsey.com/insights/business_technology/why_senior_leaders_are_the_front_line_against_cyberattacks?cid=other-eml-nsi-mip-mck-oth-1407

provide insufficient protection. And they understand that institutions need to develop much more insight into the risks they face, implement differential protection for their most important assets, build security into broader IT environments, leverage analytics to assess emerging threats, improve incident response, and enlist frontline users as stewards of important information.

The importance of cybersecurity is no secret to anyone who's opened a newspaper or attended a board meeting. So, senior executives may ask, what's the holdup? The answer is simple: understanding the issue is quite different from effectively addressing it. A number of structural and organizational issues complicate the process of implementing business-driven, risk-management-oriented cybersecurity operating models, and only sustained support from senior management can ensure progress and ultimately mitigate the risk of cyberattacks.

While progress is being made in addressing today's problems, there are a number of trends that can be expected to continue into the future should these challenges persist. These trends include the following:

- Expanding, heterogeneous user-base
- Technical innovation
- Co-evolving business practices
- Disappearing barriers between
- Networks
- Organisations
- Home, work and leisure
- Pervasive technology
- Accelerating pace of life and business
- Escalating arms race

4.1.2 Innovation Stakeholders

We now move on to consideration of the innovation/supply-side stakeholders, i.e the participants in the NIS value chain required to bring innovations 'to market'. For the purposes of this section, the term PACs (Privacy and Cybersecurity) is used to denote this market sector.

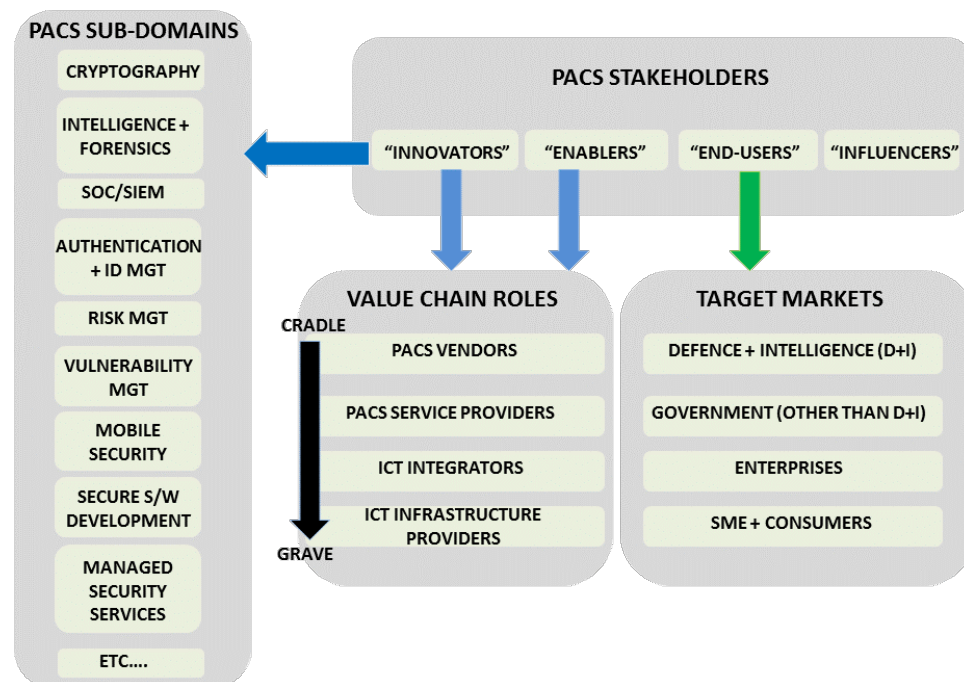


Figure 3: A schematic relationship between NIS stakeholders, NIS subdomains, key value chain roles and target market segments.

NIS innovation stakeholders can be split into four main groups:

- “Innovators” - individuals or companies that are looking to bring ideas in the NIS domain to market. Sub-categories include: Vendors, service providers, integrators and infrastructure providers;
- “Enablers” - individuals or entities who are responsible for supporting individuals in being more innovative and in commercialising technology;
- “Influencers” - individuals whose professional mandates influence or impact on the ability of NIS Innovators or Enablers to bring technologies to market;
- “End-Users” - individuals or organisations leveraging NIS technologies and services to improve resilience of their own infrastructures, or technologies they provide to others.

Different organisations and individuals may fall into multiple stakeholder categories under this scheme, depending on numerous factors, particularly their relationship with the product lifecycle. For example in relation to the development of a specific product an individual may be deeply in “Innovator” mode, whereas in terms of a strategic review their role may shift towards “Enabler” mode. Product managers in particular may have to juggle between both roles. Different innovation materials will apply to different stages of the innovation lifecycle so identifying stakeholder roles at any given time is important.

Stakeholder Type	Sub-Categories	Key innovation needs/pain points
Innovators	<p>Organisation Size/Maturity</p> <ul style="list-style-type: none"> • Academic researchers/clusters • Micro startup (1-3 persons) • Small SME (<10 persons) • Established SME seeking new business lines/opportunities • Mid-Sized company (250 employees plus) • Large global blue chip players <p>Job Title/Persona</p> <ul style="list-style-type: none"> • Product Manager • Technical Architect • Software Developer • R&D Manager <p>Target NIS Subdomain (e.g.)</p> <ul style="list-style-type: none"> • Cryptography • Intelligence and Forensics • SOC/SIEM • Authentication/ID Management • Risk Management • Vulnerability Management • Mobile Security • Secure Software Development • Managed Security Services (MSS) 	<p>Understanding the steps, procedures, activities involved in bringing new NIS product/service innovations to market – difficulty in getting NIS solution to market successfully</p> <p>Have experienced several past failures at startups and would like to learn how to avoid those failures.</p> <p>Have difficulty understanding where to prioritise and focus efforts around innovation</p> <p>Don't know how to conduct and validate market research, and integrate it with product/solution development</p> <p>Have difficulty in knowing how to access finance, both for R&D and NPD activities</p>
Enablers	<p>Typically managers or consultants working in an in-house or external support role. Can be:</p> <ul style="list-style-type: none"> • Managers with background in NIS domain, <u>without</u> expertise in general innovation techniques • General innovation consultants with no expert knowledge of NIS domain. <p>Could exist within organisation categories profiled above, from independent consultancies, VCs or similar investment agencies, NIS cluster support groups, and so on.</p>	<p>Existing NIS stakeholders will understand their domain (and often market) very well but have difficulty around building better innovation/process in the organisation.</p> <p>Difficulty in doing radical innovation well (i.e. bringing new technology to a new market)</p> <p>Want to understand how to empower other individuals and groups in organisations (i.e. innovators) – including defining roles and responsibilities for innovation activities</p>

Influencers	<p>May come from broad range of backgrounds including:</p> <ul style="list-style-type: none"> • NIS/ICT standards bodies • Data Protection Authorities • CERTs • Investors (VCs, angels, incubators etc) • R&D funding agencies (national/pan-national) • NIS market analysts (policy or commercial background) • NIS certification bodies 	<p>Understand how to build/integrate specific agenda into NIS marketplace – ensure that necessary standards/mandate are achieved</p> <p>Understand NIS trends more clearly from research and commercial perspectives (political, economic, social, technological, legal, environmental)</p> <p>Understand how role in NIS domain impacts Innovator ability to commercialise NIS technology</p>
End-Users	<p>Individuals and organisations looking to protect their business, data, operations</p> <p>General ICT vendors integrating NIS technology</p> <p>Can be further segmented by target NIS market segment, e.g.</p> <ul style="list-style-type: none"> • Defence and Intelligence • Government (excl Defence) • Enterprises • SME and consumers 	<p>Difficulty in making products, services, infrastructures secure – need security “best practice” solutions.</p> <p>How to design-in security/privacy functionality into products, services and infrastructures</p> <p>Verifying cost and risk balance around NIS. How much should be spent on NIS? How much security is enough? What is enough to keep customers/regulators happy? How might they be incentivised to adopt higher NIS standards?</p> <p>Verification of quality/effectiveness of NIS solutions they use</p>

Table 7: Stakeholder roles and innovation challenges

4.2 Approach to cost-benefit analysis of research topics

A business case is a request for funding put before an investment board or similar body. The main elements of a business case are:

- a proposal;
- an estimate of the time, resources and funding required to implement it;
- an estimate of the benefit arising as a result of implementing the proposal;
- an assessment of the risk of failure and adverse consequences.

The investment board will not disburse funding unless the estimated benefit exceeds costs by a comfortable margin. Furthermore, since the cost of proposals normally exceeds available investment budgets, the selection process typically involves ranking proposals according to some measure of net benefit, taking factors such as risk, break-even time and rate of return profile into account.

In the context of this document, the 'request' is for the allocation of a proportion of NIS research and innovation budget towards the achievement of a specified applied research goal. The potential benefit aggregates all the positive societal and economic impacts arising from the exploitation of the research resulting in products, services, solutions etc., and less tangible benefits such as public perception, societal trust, and the development of policy which cannot be valued in purely monetary terms. Even in the former case it is extremely difficult to calculate monetary gains, either direct (through solution selling) or indirect (through increased productivity). It is especially so in the case of "built in" security mechanisms that are impossible to separate from the overall ICT system.

A quantitative assessment of potential benefits of candidate research goals will often not be possible, but it is beneficial to at least articulate and assess qualitative value propositions. The creation or maximisation of value is at the heart of many innovation methodologies. In his book "Crossing the Chasm"²⁶, Geoffrey Moore²⁷ mentions that any new technology offering requires a must-have value proposition, i.e. it provides a unique way of satisfying an important requirement at affordable cost or else at significantly lower cost than the alternatives. Value creation is one of the pillars of SRI's Five Disciplines of Innovation (5DOI)²⁸ and ISACA intend their Val IT Framework²⁹ to be '*a comprehensive, credible and pragmatic organising framework—with practical guidelines, principles, processes and supporting practices that help boards, executive management and other organisational leaders maximise the realisation of value from IT investments*'.

Moore's Value Positioning Statement offers (with some minor adaptation) a template we could use for a concise high-level statement of a value proposition:

²⁶ Moore's technology adoption lifecycle recognises five main segments: innovators, early adopters, early majority, late majority and laggards. The chasm of the title refers to the difficult transition from serving early adopters to serving the early majority.

²⁷ Geoffrey A. Moore, 'Crossing the Chasm, 3rd Edition: Marketing and Selling Disruptive Products to Mainstream Customers', pub. HarperCollins, 2014

²⁸ SRI's Five Disciplines of Innovation, <http://www.sri.com/engage/innovation-programs/five-disciplines-innovation>

²⁹ ISACA Val IT Framework for Business Technology Management, <http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT1.aspx>

For <target stakeholder> in <usage or market context> who <statement of the need or opportunity> the <title of the research goal> will result in <description of a generic service, capability or enabling technology> that <statement of benefit>

The strength of the value proposition is not only a measure of the potential impact, but also affects the likelihood that the result will be taken up. Articulation of a convincing value proposition is particularly challenging in NIS, where business decision makers will not only ask questions such as “What is the value of investment in IT security?” but also “How can I be sure what is needed, efficient and effective for my IT environment?”.

NIS innovations share barriers to take up with other ICT areas (e.g. purchase budget, operational costs), but in addition there are NIS-specific barriers such as the lack of understanding, low awareness on perceived value/benefit, and the short lifecycle of security solutions (e.g. new threats appear daily, new vulnerabilities being discovered, etc.). The probability of success in developing and bringing to market research results of cybersecurity projects are therefore lower than in the most of the other ICT areas.

It is difficult to provide convincing justification for value propositions based on intangible benefits such as e.g. increased assurance, interoperability of protection mechanisms, efficiency of response, usability, etc. In addition, ROI for a strategic application or technology would be different from ROI in e.g. transformational IT. Finally, traditional ROI analyses that are based on financial models are not able to predict ROI for technologies that contain the uncertainties and trade-offs, which are intrinsic to NIS (e.g. confidentiality versus availability). This becomes an even bigger problem with the security requirements elicitation at the different levels of abstraction, especially in the privacy area.

There are, however, a number of possible ROI models that could provide the basis for ranking of research topics:

- Social return on investment model
- Value measuring methodology
- Federal enterprise architecture performance reference model
- Public sector value model
- Performance reference model
- Demand and value assessment methodology

There is furthermore a lot of research work³⁰ focused on ROI for IT security. However, when it comes to the European research projects, there are many examples that show that there is no single security ROI model. Stakeholders might invest in security depending on their threat model. Loss probability and loss

³⁰ R. Anderson, Why information security is hard — an economic perspective. 17th ACSAC, 358–365, New Orleans: IEEE, 2001.

L. Gordon, M. Loeb, Managing Cybersecurity Resources. McGraw Hill, 2006.

C. Ioannidis, D. Pym, J. Williams, Investments and trade-offs in the economics of information security. Proceedings of Financial Cryptography and Data Security '09, LNCS 5628: 148–166, 2009.

magnitude are estimated differently across sectors. While online annoyance is common, with users from all sectors or all types reporting spam or malware, actual losses are perceived differently.

Industry experts in the industry advisory focus group of the SECCORD project³¹, for example, referred to the challenge posed by value-based research projects as perhaps the single most important concern for ICT security industry organizations. Value-driven research might have dramatic implications for the R&D process, turning around how we think about “research to market” process, piloting and trials, placing the issue of “proof of value” at the start of research proposal. As such, value-driven development strategies need support and coordination that considers the ICT security solution/product **value proposition**, the **evidence** plan to support that value proposition, and the **customer acceptance** of that product and evidence when determining registration, price acceptability and market access. Understanding and managing trade-offs among these three components provides a cost, risk and return analysis that can inform the progression of research results and further investment decisions made by individual industrial partners.

If we look at the above comment that highlights the role of “customer acceptance”, it is clear that the choice of users in the research project is essential for its later success. Here, we face a major problem:

While the most EU research projects solve problems of the future and the first results are available in 3-4 years, the customer needs and expectations, especially in ICT or cybersecurity, are close to immediate. This problem deserves special support and treatment, maybe through the open calls managed by individual projects or dedicated platform.

NIS research funding should purposely target technical solutions leveraging existing technology blocks and sleeping patents.

The SECCORD results³² illustrated case studies from EU funded research projects specifically in the area of research to market propositions and their findings in relation to weaknesses are relevant to this report.

³¹ SecCord: Security and Trust Coordination and Enhanced Collaboration, an FP7 project, <http://www.seccord.eu/>

³² SecCord Deliverable pg 91 Success Stories <http://www.cspforum.eu/Yearbook2013-V1.42.pdf>

The R&D projects often do not execute market studies for their technologies and do not take costs into account to ensure acceptance of their technology. The business model says security must also be economically viable.

4.3 Market demand and high impact use cases

Appendix E contains a collection of descriptions of scenarios with challenging security requirements proposed by contributors to this study, such that meeting those requirements will have significant societal or economic benefit. It is important to remember that these are use case scenarios and not descriptions of research topics. The idea is that we will end up with a list of research goals that can be justified (at least in part) because they are derived from (and can be traced back to) high-priority security requirements that are currently not met. Thus the logic of this part of the report leads from stakeholder concerns, to use cases that make those concerns concrete in specific scenarios, to capabilities/services that would address those concerns, from which we can define research goals by generalisation or identifying enabling advances. Note that ideally there would be a many-many relationship between scenarios and research goals, and research goals that affect multiple scenarios will be ranked higher in terms of impact.

The following was the guideline given for the contents and structure of a use case description, though not all contributions follow it rigidly:

1. Description of setting
2. Dramatis personae (description of stakeholders and threat agents, etc.
3. Main security concerns of stakeholders that are currently addressed inadequately
4. New (hypothetical/abstract) services that would solve the problem
5. Required enabling technologies / capabilities
6. Assumptions / dependencies

The use cases are not intended as a complete set of security scenarios, rather, they are a collection of representative examples from which we can generalise.

4.4 Example research topics and value statements

Appendix F outlines a selection high impact security research topics justified by value statements. Each research topic should describe a requirement for an 'artefact' (e.g. a service, capability, reference framework, technique, enabling technology, etc.) that will be valuable in multiple usage contexts envisaged for around 2025. They should not be proposals for specific implementations of the artefacts. They should reference applicable use cases from the previous step in the methodology or other stages.

They topics are grouped according to a number of major categories of artefact we have identified.

- Security services and capabilities
- Trusted and resilient infrastructure
- Secure software/systems engineering methods and tools
- Security management solutions

While we do contend that the topics described are potentially 'high impact', they should be regarded as examples that have come up in the course of the study and not as an exhaustive list. The current topic descriptions are few in number, vary considerably in maturity, and have not been evaluated critically and ranked by the group as would normally be done in applying the methodology.

4.5 Next steps

Steps required to conclude the process begun here are listed below. Time did not allow us to complete the example application of the methodology to the depth originally intended. Remaining steps to illustratively establish the viability of the approach so that it may be continued are as follows:

1. The current set of use cases needs to be refined and brought to a uniform standard in which specific scenarios are analysed to draw out services/capabilities/enabling technologies required to satisfy stakeholder needs in that setting.
2. Further use cases should be identified and developed until there is a reasonable coverage of the range of future application domains (taking into account the output of the WG3 Area of Interest groups).
3. If time allows, particular use cases will be highlighted for more detailed study.
4. The work initiated on the goal-oriented research topics should be continued and aligned with the use cases such that the degree to which the topics are justified by demand stakeholder requirements can clearly be seen. A shortlist of topics would then be drawn up taking into account linkage to requirements. We will take into account sources such as the WG3 Secure ICT Landscape deliverable and the output of CAPITAL and other projects.
5. This shortlist of topics would be further analysed and consolidated to obtain a recommended 'portfolio' of research investment opportunities justified in qualitative cost-benefit terms.

5 Process Definition & Innovation Models

5.1 Introduction

Processes for fostering and managing innovation are essential to the maintenance of economic growth at the organisational level, as well as at national and international levels. The challenges inherent in the globalisation of competition mean that effective innovation has become critical. This chapter will begin by giving a brief overview of Innovation models outlining the six generations of innovation models ranging from the first generation, started in the 1950's to the contemporary model of open innovation. Each generation will be outlined with the changes and developments evident. The basis for this is Rothwell's (1994) five generations of innovation models which range from the relatively simple linear models of the first two generations, to the more complex fifth generation model which includes real time feedback loops and complex integration both between and within firms. The final innovation model is the Open Innovation model, which expands on Rothwell's previous models while maintaining a focus on openness and the sharing of knowledge and information both within and between various organisations. After elucidating these models of innovation this chapter will progress to give applied examples of how innovation is fostered and managed within companies. The organisations which have contributed their case studies include; BT, ENG, Espion, ATOS, HP, SAP, Technikon and LSEC. Following on from this, the chapter will progress to further discuss best practice recommendations including the example of European Institute of Innovation and Technology (EIT) ICT labs and the Knowledge Innovation Community (KIC). One of the core problems identified in technological research and innovation is that of technology transfer which is concerned with the transposal of the outputs of research and innovation to the marketplace. High-level recommendations are proposed to address this challenge.

The methodology adopted for the Process Definition & Innovation Models is as follows:

1. Analyse existing innovation models and processes and recent trends within the literature.
2. Aggregate common and best practices in research and innovation (R&I) relevant to cybersecurity, drawing on a wide range of sources including success/failure stories from past projects, the output of co-ordination actions and projects, journal papers and articles, case study material direct from contributing organisations and supporting national and European innovation agencies.
3. Drawing upon the collected data, define a shortlist of alternative / complementary end-to-end R&I process models, identifying the stakeholders involved.
4. Analyse the shortlisted models and practices (e.g. using a SWOT – strengths, weaknesses, opportunities, threats – approach). Identify potential mitigations for the threats to the R&I models (e.g. education/training/transfer programmes to provide specialist skills, economic incentives, research infrastructure, etc).

5. Recommend (with justifying arguments) one or more R&I process models for adoption in future programmes, together with supporting actions required to improve their prospects of success.

To date we have completed steps 1 and 2 above within the first phase in this process and have collected much of the relevant data with initial recommendations and findings.

Section 5.3 and section 5.4 present innovation models and best practices from academia and industry that can be applied to research and innovation in cybersecurity. Drawing on research from the European Commission FP7 funded SecCord research programme (Kapletia, et al. 2014), it is useful to start with a holistic end-to-end view of the innovation management landscape, as outlined below in Figure 2 which is a Logic model for innovation management in cybersecurity. In the context of increasing the impact of publically funded research and development (R&D) in cybersecurity, the diagram proposes three main focal areas, (I) R&D market and policy, (II) Technology readiness, and (III) Technology transfer. This reflects the broad process from early stage funding decisions, through to full technology readiness and successful operational application. The original diagram has been modified to illustrate the scope of stakeholders influence and interests from section 4.

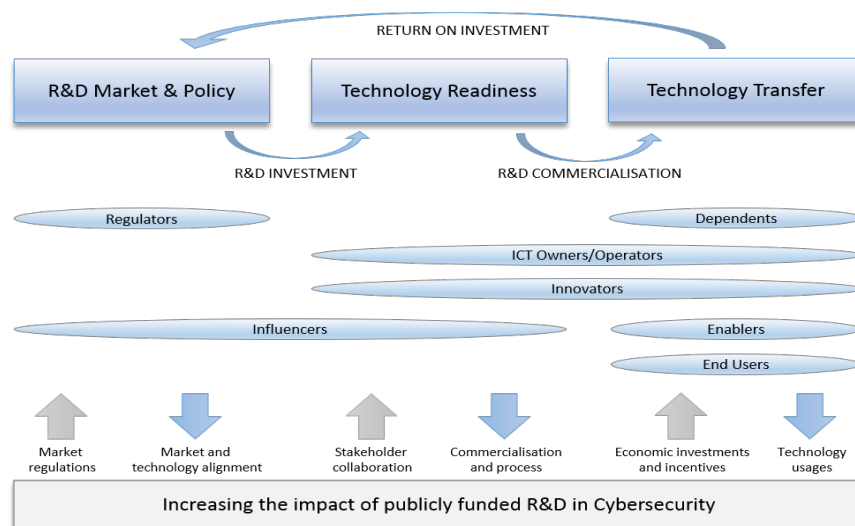


Figure 4: Logic model for innovation management in cybersecurity, modified from Kapletia et al. (2014)³³

The innovation models and best practices presented in this section illustrate the variety of approaches that can be adopted. This includes both a review of academic thinking and perspectives from government and industry players. It is useful to consider the bigger picture of how approaches to innovation have evolved alongside investments and decisions required at the operational level. However, a

³³ Kapletia, D; Felici, M; and Wainwright, N. (2014) Towards an integrated view of innovation management in cybersecurity, paper presented at SecCord CSP Forum in Athens in May 2014

prescriptive approach to managing innovation is unlikely to work for cybersecurity due to the diversity of organisations and operating environments involved.

5.2 Contextual considerations

The concepts discussed in this section reflect the specific kinds of organisations, SMEs, Universities and global corporations contributors from the working group, representative of a sample of stakeholders. Specifically a number of organisations; BT, ENG, Espion, ATOS, HP, SAP, Technikon and LSCE have provided examples of how innovation is managed in their respective organisations. Using these case studies as examples, there are a number of useful considerations that have been identified, these include:

- Extent of internal and external collaboration, using open vs. protected approaches
- Key commercial activities/milestones required across the lifecycle in figure A, from pre-R&D to post R&D
- Investment in business disciplines conducive to successful innovation
- A top-down versus bottom up approach to R&D
- Mapping technical offerings against applications and market demand
- Early stages of analysing ideas/concepts and critiquing their associated risks and application potentials
- Understanding and overcoming the tensions between research and innovation
- Value and use of formal centralised new product development processes versus an unstructured ingredient-based approach
- The role and scope of policies, organisations and teams charged with finding commercial routes and applications for new technologies
- The different types of individuals and skills-sets required at different stages of R&D
- Enablers and barriers applicable to innovation in cybersecurity R&D

5.3 Innovation Models

Understanding of the process of innovation at the firm-level has evolved throughout recent decades from simple linear and sequential models to increasingly complex models embodying a diverse range of inter and intra stakeholders and processes. Distinguishable by their management focus, strategic drivers, accommodation of external actors and internal and external processes and function level integration,

Rothwell (1994)³⁴ documented 5 shifts or generations, which are simplistically depicted by Cagnazzo et al. (1998)³⁵ in Figure 5 below.

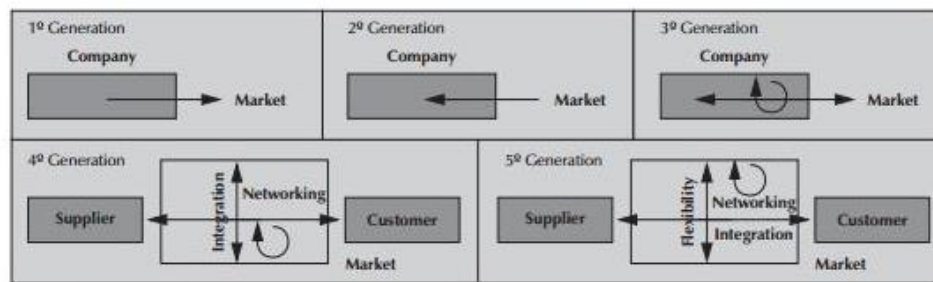


Figure 5: Five Generations of Innovation models

Rothwell's (1994) classification of innovation models demonstrates that the complexity and integration of the models increases with each subsequent generation as new practices emerge to remedy the shortcomings of earlier generations and to adapt to a changing context (Ortt and van der Duin, 2008)³⁶. Before examining individual models, it is useful to emphasise the following caveat - the evolving generation of innovation models does not imply any automatic substitution of one model for another; many models exist side-by-side and, in some cases, elements of one model are interweaved with elements of another. Table 8 below identifies the various generations by their type and describes each of them using distinguishing characteristics.

³⁴ Rothwell, R., (1994) Towards the fifth-generation innovation process. *International Marketing Review* 11 (1), 7–31. <http://www.sri.com/engage/innovation-programs/five-disciplines-innovation>

³⁵ Cagnazzo, Luca; Taticchi, Paolo; Botarelli, Marco. (2008). "A literature review on innovation management tools". *Revista de Administração da Universidade Federal de Santa Maria*, num. Septiembre-Diciembre, pp. 316-330.

³⁶ Ortt J.R. and van der Duin P.A. (2008) "The Evolution of Innovation Management towards Contextual Innovation", *European Journal of Innovation Management*, 11, p. 522-538.

Characteristics	Type of model		
	<i>Linear</i>	<i>Interactive</i>	<i>Integrated</i>
Timeframe	1950s to late-1970s	Mid-1970s to mid-1980s	Mid-1980s-present
Generations (model exemplars)	First Generation (Technology-Push); Second Generation (Market-Pull)	Third Generation (Chain-Linked)	Fourth Generation (Cooperative R&D); Fifth Generation (Systems Integration and Networking; SIN)
R&D	An increase in R&D results in more innovation output.	Emphasises how R&D interacts with market forces.	Emphasises cooperative R&D and the links between independent agents.
Knowledge source	Internal scientific research is the main knowledge source.	Internal scientific research as well as knowledge acquired from other (mainly) internal sources.	Knowledge acquired from both internal and external sources.
Market forces	For technology-push the market forces are largely ignored. For market-pull the market forces direct the R&D investment.	Market forces interact with R&D decision-making.	Horizontal and vertical alliances respond to market changes.

Table 8: Classification of Innovation models

Building on the seminal categorisations of Rothwell (1994)³⁴, other researchers have suggested the existence of 6th generation innovation models. For instance, Kotsemir and Meissner (2013)³⁷ suggest that Chesbrough's (2003)³⁸ open innovation model represents the latest generation of innovation modelling.

5.3.1 First Generation- Technology Push (1950s to mid 1960s)

This era of innovation models represents a simple linear structure which treated innovation as a sequential process performed across discrete stages. Technology push is based on the assumption that new technological advances based on R&D and scientific discovery, preceded and 'pushed' technological innovation via applied research, engineering, manufacturing and marketing towards successful products or inventions as outputs.

³⁷ Kotsemir M. N., Meissner D (2013). [Conceptualizing the innovation process – trends and outlook](#) / Working papers by NRU HSE. Series SCIENCE, TECHNOLOGY, INNOVATION "SCIENCE, TECHNOLOGY, INNOVATION". 2013. No. 10/STI/2013.

³⁸ Chesbrough, H. (2003), *Open Innovation: The New Imperative for Creating and Profiting from Technology*, Harvard Business School Press (2012)

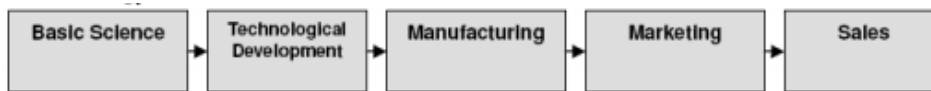


Figure 6: 1st Generation Innovation model

5.3.2 Second Generation – Market Pull (Mid 1960s to early 1970s)

In this generation a linear model of innovation also applies, this time prioritising the importance of market demand in driving innovation endeavours. What distinguishes this model from the previous model was that rather than product development originating from scientific advances, the new ideas originated in the marketplace, with R&D becoming reactive to these needs.

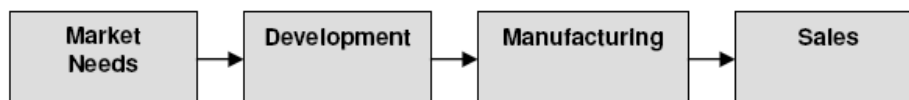


Figure 7: 2nd Generation Innovation model

5.3.3 Third Generation – Interactive, Coupling or Chain-linked models (Early 1970s to mid 1980s)

The third generation model overcame many of the shortcomings of the previous extreme and atypical examples models, by building in interaction and feedback loops to recognise that innovation is characterised by a coupling of and interaction between science and technology and the marketplace. Consequently, the model integrates multiple in-house functions and interdependent stages and introduces a role for external stakeholders beyond the organisation (for example, customer and supplier relations).

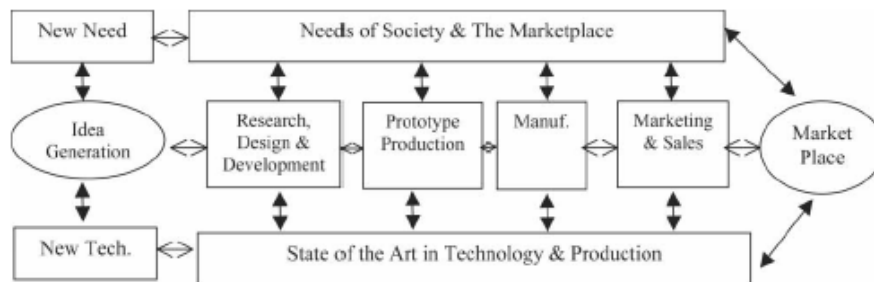


Figure 8: 3rd Generation Innovation model

5.3.4 Fourth Generation – Integrated model (Early 1980s to early 1990s)

While third generation models were non-linear with feedback loops, a sequential nature of the stages of innovation were characterised. In response, and aiming to reflect the high degree of cross function integration within firms, integrated or parallel models began to be developed that involved significant functional overlaps between departments and/or activities. A further novel feature of this model is the concept of external integration in terms of alliances and linkages with suppliers, customers, universities and government agencies.

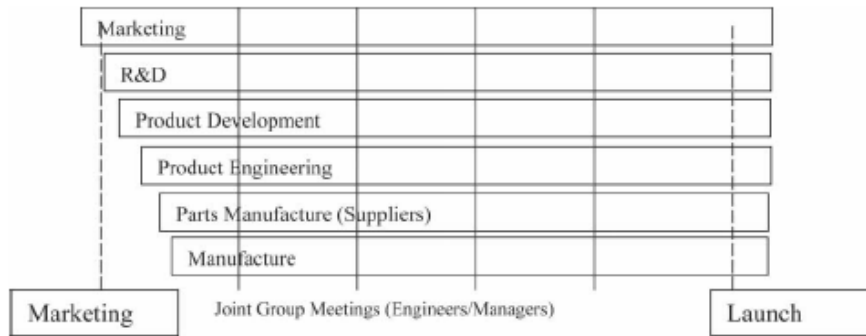


Figure 9: 4th Generation Innovation model

5.3.5 Fifth Generation – Systems integration and network model

Extending from the previous generation of innovation models, systems integration and networking models emphasise that innovation is a distributed networking process requiring continuous change occurring within and between firms characterised by a range of external inputs encompassing suppliers, customers, competitors and universities. Reflecting a systems thinking approach, the dominant characteristics are the integration of a firm's internal innovation ecosystem and practices with external factors in the National Innovation Environment. The fifth generation model is characterised by the introduction of ICT systems to accelerate the innovation processes and communications across the networking systems in terms of raising both development efficiency and speed-to-market through strategic alliances.

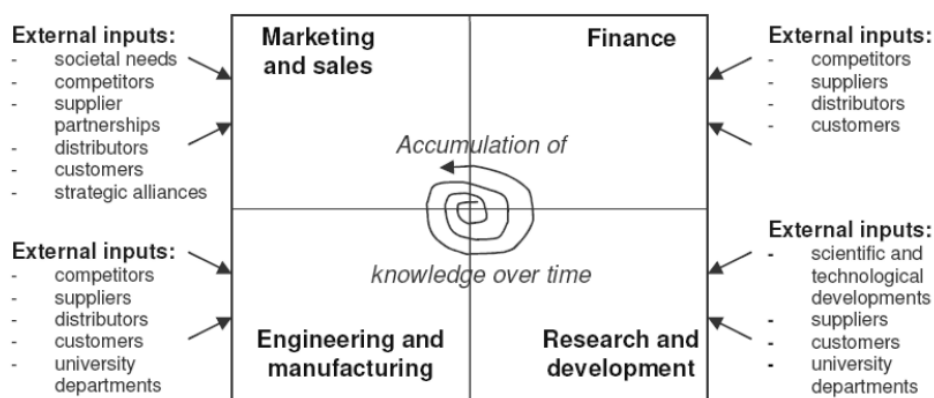


Figure 10: 5th Generation Innovation model

5.3.6 Sixth Generation Open Innovation Models

More recently and following on from the seminal work of Rothwell's (1994)³⁴ innovation generation model typology, researchers Kotsemir and Meissner (2013)³⁷ have suggested that Chesbrough's (2003)³⁸ open innovation model represent the latest wave of innovation models. Reflecting a dominant orientation to the preceding network models of innovation, the open innovation is not limited to internal idea generation and development, as internal and external ideas in addition to internal and external paths to market are facilitated to advance the development of new technologies.

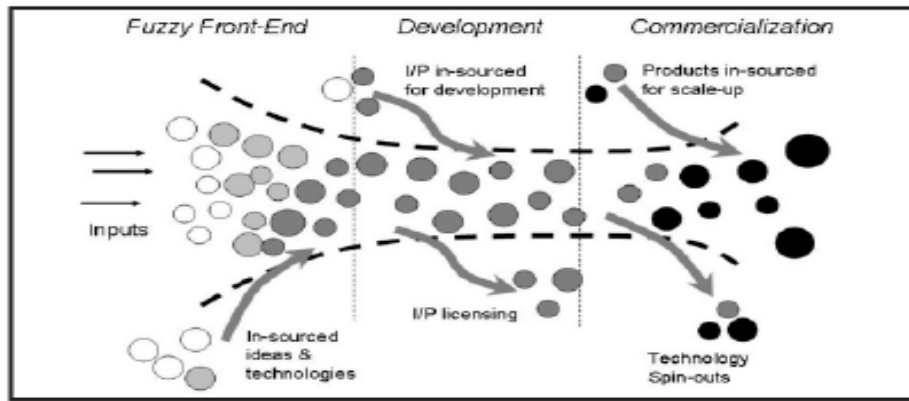


Figure 11: 6th Generation Innovation model

5.3.7 Conclusion

This section has sequentially examined the main innovation models in a manner, which facilitates comparisons between them from a historical perspective. It has traced the contours of change which are inherent in the movement from early generations which were insular, linear, and reactive models of innovation towards the more contemporary models which are fluid and adaptable processes which aim to raise development efficiency and speed to market through inter-organisational cooperation and strategic alliances. The most recent models of innovation are those that are based around the idea of a distributed networking process, which is ever changing and so is well positioned to absorb and react to any changes in material market conditions. Now that these archetypical models of innovation have been examined; it is necessary to attempt to examine the application or otherwise of these models in real world examples. The following sections involve descriptions of the innovation processes and procedures employed by eight companies namely BT, Eng, Espion, ATOS, HP, SAP, Technikon and LSEC. The CYSPA project further argues the strengths and weaknesses of the discussed models and complements the findings and recommendations herein this report while mapping their examples of in-house innovation methods to the theoretical models.

5.4 European and US approaches to innovation in technology

This section will outline existing best practices in research and innovation with a particular focus on technology. The information presented is drawn from a variety of sources including contributed case studies from particular companies, academic papers and reports focused on innovation in technology. The companies to be described are BT, ENG, Espion, ATOS, HP, SAP, Technikon and LSEC. Appendix B outlines the US department of homeland security R&D Innovation model. The different pathways to innovation are examined and in each case the ideas and practices involved in the process of fostering innovation are explained.

5.4.1 Research and Innovation in BT

Research and Innovation are two distinct, but coupled processes. One way of explaining the difference is to say that while research is concerned with turning money into new knowledge; innovation is concerned with turning new knowledge into money or other forms of value. The scope for innovation is limited without research programmes to generate intellectual capital. Conversely, without the process of innovation, many of the potential benefits of research will not be realised.

BT practices Open Innovation, which means that it draws upon a variety of sources of new ideas and enabling technology. These include its internal applied research capability, the Research & Technology department (R&T), which is organised into a number of research practices, one of which is focused on security research. R&T performs both internal and collaborative applied research, and also has access to more fundamental research results via strong relationships with leading universities. The research programme is funded and overseen by the BT Research Investment Board (RIB), which includes representatives from BT's lines of business, ensuring that research is focused on business- relevant topics.

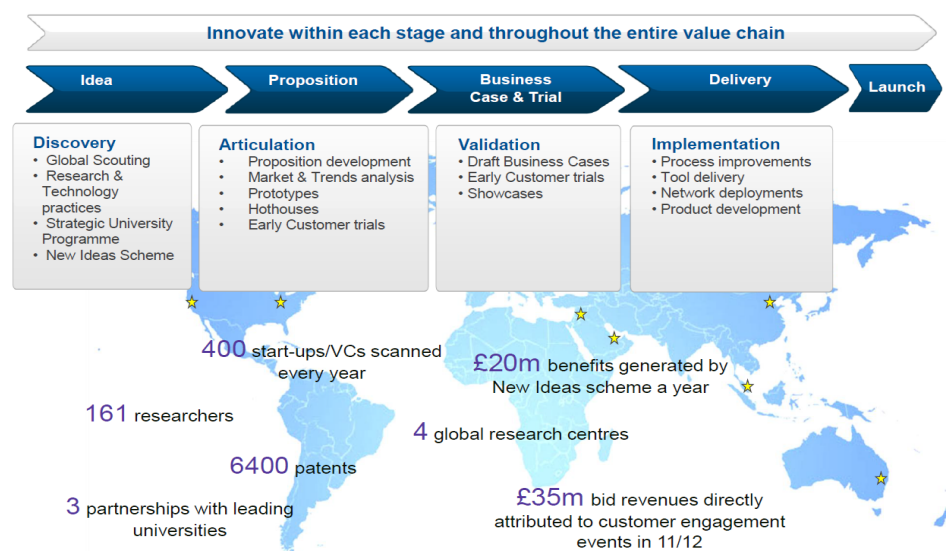


Figure 12: BT's Innovation Process

BT's Innovation Process (see Figure 12) has four formal stages:

1. **Idea:** This involves the identification of potential innovations, typically bringing together a new technology, technique or way of working, with a business need that is aligned with BT's Strategy and Portfolio. These ideas can come from a number of sources, including:
 - a) Co-creation with customers, facilitated by 'hothouse' and other events
 - b) External partners, which could be major industry players, or recent start-ups with potentially disruptive technology or business models revealed by the Global Scouting function
 - c) Non-research employees, e.g. via the New Ideas Scheme
 - d) The internal research programme

e) Academia

2. **Proposition:** Here, the idea is articulated as a business proposition, answering questions such as 'What is the value proposition?', 'Who sells what to whom?', 'Who are the competitors?', 'Why can BT do this?' This stage may involve producing demonstrators and performing preliminary customer trials to test and refine the proposition.
3. **Business Case and Trial:** If the proposition is judged to be sufficiently strong, then the size of the opportunity is quantified, the required investment and resources estimated, and a business case drawn up. Further customer trials and showcase demonstrations may take place to support this activity.
4. **Delivery:** If the investment identified in the business case is approved, the product/service/process improvement is developed, implemented and deployed. This completes the innovation process and the next step is a launch decision.

5.4.2 Research and Innovation in Engineering Ingegneria Informatica S.p.a (ENG)

To analyse the R&I process within ENG, the following picture provides an overview of the structure of the company, an overall group of 7.500 employees and consulting personnel.

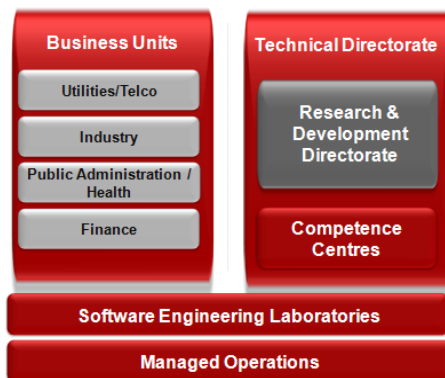


Figure 13: Organisational structure of ENG

The **Business Units** are in charge of the following business functions:

- the sale of products, services and projects in different market segments;
- expertise on different fields of application domains;
- technical and contractual management of projects and services provided to clients;

The **Technical Directorate** has two units, which are in charge of the following business functions:

- defining the architectural and technological solutions offered on the market
- implementing research projects in accordance with the strategic innovation (this function is entrusted to the Research & Development Directorate);
- transferring the technical know-how to the Business Units through the Competence Centres

The **Software Engineering Laboratories** are devoted to software development according to the company's production process. They work closely with the

Technical Directorate for technical and architectural choices for the implementation of projects.

Managed Operations is the directorate in charge of managing corporate data centres that provide outsourcing services systems for customers. ENG currently operates 5 centres, coping with 15.000 servers and 230.000 workstations over 7.400 m².

The following figure schematically shows the relationships that exist among the different corporate directorates with respect to the **research and innovation**.

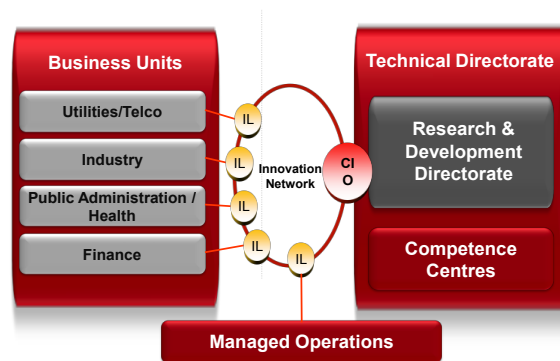


Figure 14: R&D within ENG

The **Research & Development Directorate** is in charge of the technical guide of all the research and innovation. These activities must take into account:

- technological trends,
- market demands
- corporate strategies.

In order to make a proper review of these requirements, an Innovation Network has been created, to which all corporate units/directorates take part with a representative (Innovation Leader). The Innovation Network is coordinated by the Research & Development Directorate through the **Chief Innovation Officer (CIO)**.

Each **Innovation Leader** is in charge of:

- meeting the specific needs of innovation coming from the Business Unit to which it belongs;
- developing a plan of innovations gathered;
- submitting that plan to the Innovation Network.

The role of the Chief Innovation Officer is to:

- collect different levels of product innovation by Innovation Leaders;
- coordinate a discussion on the different innovation plans to achieve a shared plan;
- draw up the innovation plan that is then submitted to the executive management level (CEO and General Managers/Directors of Business Units).

After approval of the plan, the Chief Innovation Officer, together with the R&D Directors, decide which research projects will be part of the plan itself.

This process aims to create a virtuous circle between research and its impact on the market, due to:

- all the units/directorates involved in the business processes are also involved in drafting the plan of innovation
- each Business Unit can contribute to the needs of the market in which it operates through the Innovation Network
- the process of plan development is guided by the Research & Development Directorate; in this way, the final plan combines the needs of Business Units with the state of the art of technological research
- research projects that implement the plan are carried out under the guidance of the Research & Development Directorate with the participation of other corporate functions: Managed Operations, Business Units and Software Factories, depending on the specific project. The research projects can also be used to create early collaboration with potential clients who join the consortium as users (in requirements, validation and / or piloting phases).

Once the project gets technical approval as described above, the related necessary investment goes to the final approval by the General Directorate which will take the investment in charge, then to the CEO, or the Board of Directors, depending on the total amount.

The impact of the research results on business growth is estimated through the analysis of the percentage of the revenues generated in for example, 2010 and related with the adoption and transfer of results coming from technological research on the different business sectors. This estimate has highlighted that more of the 40% of the revenue generated in 2010 is related to the results and competencies coming from technological research made in the last 5 years.

5.4.3 Research and Innovation in Espion

Company Overview: Founded in 2001, Espion are a fast growing Irish-owned SME in the Information Security and Digital Forensics/eDiscovery space, with presence in Ireland, UK and mainland Europe, with a current headcount of 80 employees. The company operates across six key business divisions, with activities ranging from consultancy and solution delivery in IT Security, Information Governance, Digital Forensics and eDiscovery, technology distribution of leading-edge security and networking products, managed security services, training and R&D.

Espion operates in Ireland, the UK and mainland Europe with clients spanning sectors including financial, retail, e-Commerce, government and legal among many others. Domestically, Espion works with six of the top 10 banks in Ireland and three of the five largest retailers.

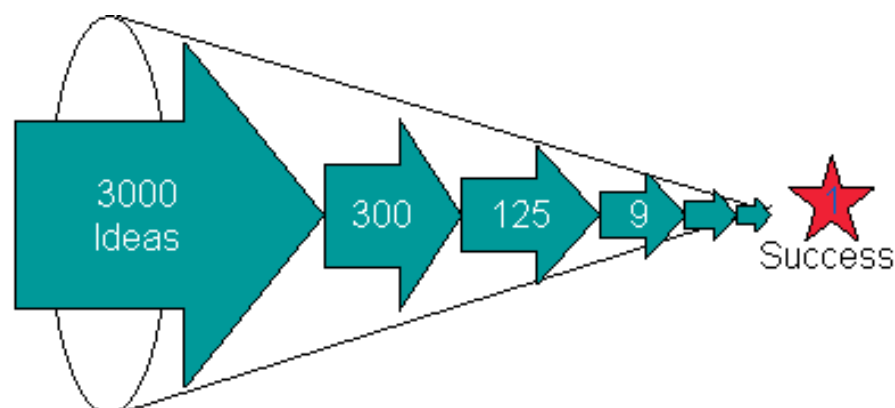
Espion and Innovation: Espion wishes to leverage innovation and R&D best practices to support next stage company growth, shifting the company from its present consultancy/service focus towards greater emphasis on developing its own solution technologies, and targeting opportunities both within and beyond its current areas of focus. This has led to increased investment in R&D initiatives, including participation in EU Framework projects, namely SAWSOC (focus on correlation of physical and logical security technologies), ECOSSIAN (focus on cross-border

security information sharing), IPaCSO (innovation frameworks for privacy and cybersecurity), and CAMINO (R&D roadmap development for cybercrime and cyber terrorism). Espion intend to develop new technology, knowledge and skills assets as a by-product of this investment in EU research activity.

Complementing this R&D activity is the goal of integrating more explicit innovation management procedures across the entire organisation, supporting incremental innovation and process improvement within the existing divisions, as well as targeting structured identification, assessment and commercialisation of new technology development opportunities. Hence, given that this initiative is still at an early stage, many innovation issues of relevance to Espion at present relate to broader structural innovation issues rather than specific micro issues at the product/technology development level, which will have parallel priorities at a later stage. Key innovation issues for Espion in the near term include:

- Increasing formal innovation training, awareness and understanding across the growing organisation, involving all employees with different operational priorities from an innovation process
- Structured and repeatable procedures and initiatives around idea generation, particularly in relation to external customer and stakeholder engagement
- More formal procedures around resource/budget allocation and its prioritisation for an agreed portfolio of innovation projects
- Developing clear incentive schemes for employees to improve their interest and engagement in innovation projects
- Managing potential conflicts of interest between divisions so that time for more strategic innovation projects is made available alongside day-to-day operational issues

Investment is also presently being made in advance of anticipated future technology and product development, with new personnel with technology product management skillsets being brought into Espion's team as well as existing key



personnel being upskilled to facilitate this transition.

Figure 15: ESPION innovation process

5.4.4 Research and Innovation in ATOS Research & Innovation (ARI)

ATOS apply both top-down and bottom-up modeling paradigms, used to emphasise and distinguish different approaches to innovation processes such as analysis/synthesis structures or in our case, focused on successful innovation and

technology adoption (market-driven innovation). In the area of “ARI research to market” technology transfer, the top-down part refers to client demand and market maturity, while bottom-up corresponds to the idea-driven or curiosity-driven research situations (e.g. innovation funnel).

Top-down models also examine the broader societal issues and incorporate feedback effects triggered by policy-induced changes, but typically do not feature technological details. As an example we show below a figure from Atos Ascent Trend analysis that can be freely accessed through <http://ascentlookout.atos.net/>

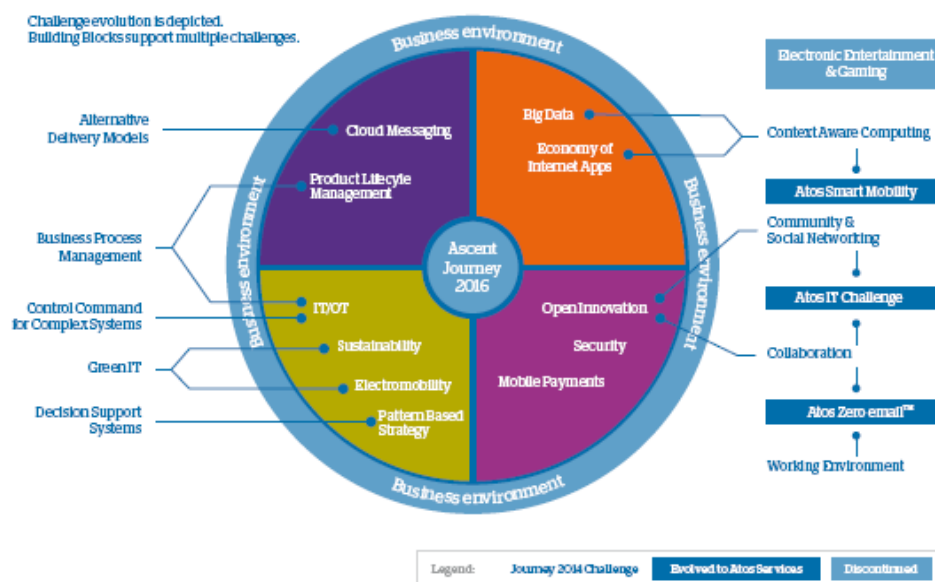


Figure 16: ATOS Innovation process

As well as these top-down assessments and technology radars, there is also strategic roadmap planning that includes white paper drafting, as well as short term roadmaps and proof of concept (PoC) pilots which are financed internally³⁹.



Figure 17: Different levels of innovation

However these pilots have weaknesses and they can also fail to capture the richness of alternatives such as emerging research community outputs and out-of-box thinking. In contrast, bottom-up approaches and collaborative research projects

³⁹<http://atos.net/en-us/home/we-are/ascent-thought-leadership/ascent-white-papers-form.html>

have more focus on ideas and technologies, as well as specific research gaps. They are therefore well suited for the more risky type of projects and more generic technological challenges, although they might fail to have high impact on market adoption or Atos innovation process. This problem of crossing the gap between research and market is depicted below in Figure 18.

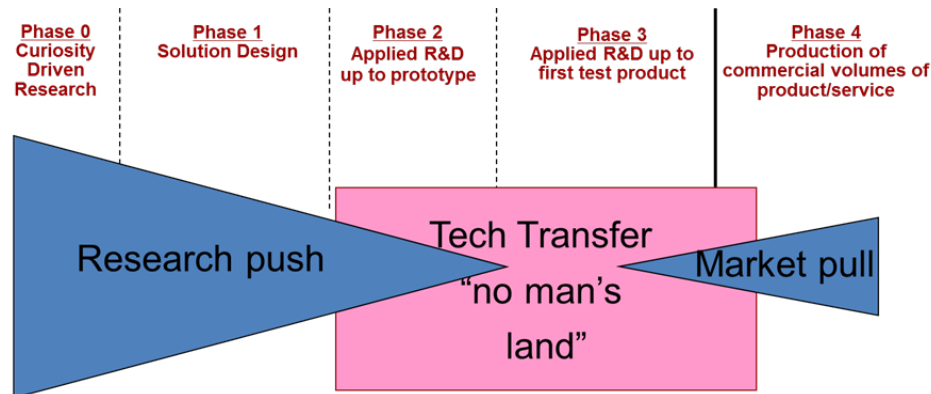


Figure 18: Research and market gap

There are several hybrid-modeling efforts that aim at combining the technological richness of bottom-up models with the market, economic, and social requirements, which come from top-down models. These efforts can be broadly classified into two approaches, which are the soft and hard mapping approaches. Soft mapping approaches face substantial problems in dispersion of attention and achieving overall consistency or convergence. Hard mapping approaches alternately might fail to capture the richness of all possible applications for a specific innovation or research outcome (e.g. software component). Atos Research & Innovation (ARI) market managers are in continuous contact (commercial committee is held every 2 weeks) with their Atos counterparts (local and global) in order to have good overview of situation at the market and to avoid the above named problems of soft and hard mapping between technical offerings and market demand. After segmentation and filtering, the list of possible users (e.g. PoC pilot, first deployment) can be made and sales people can begin to be involved in the next steps, which could include organising innovation workshops or customer presentations.

The bottom-up part of Atos Research & Innovation ARI methodology uses different tools such as the "idea generator" tool⁴⁰, idea maturity assessment, online surveys, and the workshops. These have been consolidated into in a number of relevant research driven bottom-up topics which have priority and possible impact indices. The consequent phases of this methodology are oriented towards the design of a solution (e.g. integration in the existing portfolio of ARI or global key offerings of Atos) and prototyping. While the final phase considers mapping to "top-down" issues such as market demand, aimed at the integration of research results into commercial offers.

⁴⁰ <http://pgi2.es.atos.net/node/236>

Sandclock methodology © was developed by Atos in order not only to cross this “no man’s land”, between research and market, but also to widen the most narrow part, the bottleneck, and to enable sand to flow smoothly in both directions.

The methodology is supported by a number of tools and templates, such as value proposition dialogue, so that the right, user-driven focus is given from the outset of a research project. ARI has developed a methodology⁴¹ which is building a value proposition and business case scenario, based on the deconstruction of the value chain.

Once that value proposition is selected, the project result scoping, and Atos positioning has to be negotiated within the consortium. This obviously only applies if the project is executed within a collaborative research context. Related activities include the drafting of research result definition, positioning, and a “light” SWOT analysis. Strategies of exploitation are selected at this research proposal stage’ these strategies can be incremental (asset/solution improvement through the new project), puzzle/mosaic (each solution component is developed in a different project) or disruptive (asset/solution developed from scratch, this is justified in the case of a huge market potential). This usually also involves the legal department, since IPR, previous results, and licensing issues among others have to be discussed. Early and iterative prototypes are considered important aspects to be negotiated within the consortium.

Other issues addressed at this stage, jointly by research and market teams, include risk assessment for technology transfer, namely

- Fragmentation of ownership
- User requirements that do not adapt to project lifecycle and needs
- Assumptions and simplifications done in the research project
- Lab versus operational environment
- Maintenance issues (know-how, costs etc.)

The joint ownership model at ATOS in relation to the merger of ARI asset and/or Atos GKO (global key offering) marketing and project dissemination activities particularly in the market positioning of “beta” versions and project announcements is key in the project advancement to market. The involvement of different teams is depicted in the following diagram.

⁴¹<http://es.scribd.com/doc/66408751/Identification-of-Business-Models-Through-Value-Chain-Analysis-A-Method-for-Exploiting-Large-Technology-Projects-A-Whitepaper>

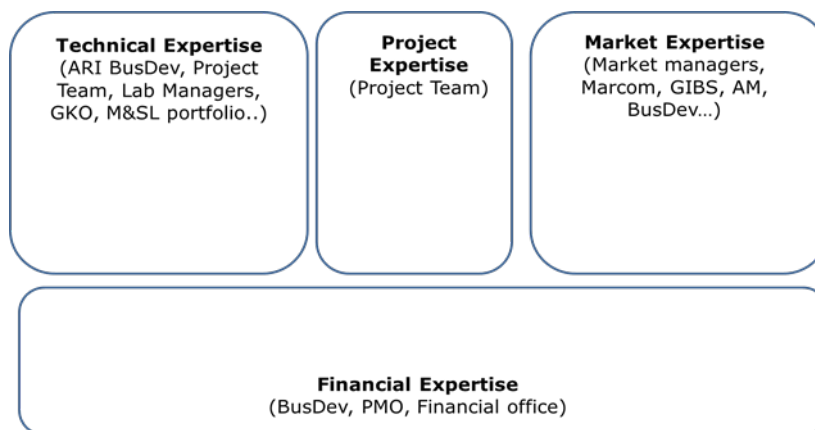


Figure 19: Cross-team innovation fertilisation

A focused approach to business modelling has resulted in six recommended models for charging customers on cloud services; these are the subscription model, the metered model, the transaction-based model, the revenue sharing model, the freemium model or the advertising-supported business model. In addition, Atos service line have their own revenue models such as a fixed daily fee for consulting services/system integration or an annual fee for managed operation/hosting services.

Cost Structure is also part of a “generic” package provided by ARI BusDev that can be customised for each set of project results. There are categories generic to the exploitation of project results, such as infrastructure costs (incl. facilities), development and deployment costs, and labour costs. When applicable the cloud model is the preferred option for the exploitation of results. In this model, the various factors of operation can be shared, and the operational costs will be lower through economy of scale. The other costs incurred from supporting services, marketing costs etc. are also included.

5.4.5 Research and Innovation at HP

Hewlett-Packard (HP) is actively involved in both exploratory research for ‘revolutionary’ innovations and ‘developmental’ evolutionary innovations. HP Laboratories sits within the corporate function and leads the longer-term (5-20 years) applied and exploratory research, whilst the business units run their own (closer to market) technology development activities. Table 9 points out some of the distinctions, and the following review provides an outline of how innovation is perceived and practiced within HP Labs and HP business units.

Business sustaining evolutionary innovations (HP business units)	Disruptive revolutionary innovations (HP Labs)
<p>Addresses existing markets, improving value and competitiveness</p> <p>Can be evolutionary or revolutionary</p> <p>Whitespace is a quick win in an area of adjacency or extension; the sum is more than the parts</p> <p>Short-term: faster ROI, incremental impact.</p>	<p>Displaces existing markets, creates new markets, values and competitiveness</p> <p>Introduces new technologies, products or services</p> <p>Whitespace is an opportunity no one else sees or can address</p> <p>Longer-term: higher risk/return, potential for advantage and differentiation</p>

Table 9: Innovation horizons at HP

HP Labs is involved in a continuous process of reviewing where to focus its innovation efforts. Currently, the focus is on cloud, security, big data and mobility. For new innovations, (looking internally) it is important to consider achieving integration across technology components, systems and/or solutions; and (looking externally) it is necessary to consider integration with wider ICT ecosystems.

New innovations in HP are commercialised through a number of routes, these include:

- Technology transfer
- Supply chain
- Licensing
- Enterprise services
- HP IT
- Incubations

At HP Labs, there is less focus on a linear innovation process, rather successful innovation is considered to involve a complex formula of ingredients. These include (I) diverse perspectives, (II) co-innovation with customers, (III) interdisciplinary curriculum, (IV) global talent development, and (V) skills for disruptive innovation. Points one to four are self-explanatory. For the last point, skills required for achieving disruptive innovation include pattern recognition, visualisation, observing and questioning, experimenting, and networking.

The focus on human talent is a critical factor for both disruptive and evolutionary innovations. This point is also drawn out in an article by Rivas and Gobeli (2005)⁴², which provides a number of interesting insights from their critique of innovation

⁴² Rivas, R; and Gobeli, DH. (2005) Accelerating Innovation at Hewlett-Packard, Research Technology Management, Jan-Feb, pp. 32-39

management at one of Hewlett-Packard's (HP) US technology development centres (inkjet related business unit).

Adopting a structured case approach, the study examined seven R&D programmes and interviewed 21 staff. Based on the historical experiences of these staff, the objective was to characterise key innovation process 'enablers' and 'barriers', and deliver recommendations for improving the management of innovation throughput. The following innovation factors from the literature were employed to generate insights from interviews with HP staff:

1. Checkpoint processes – use of staged phase/gate models
2. Integration team – issues around technology selection and integration, as well as team structures, composition, size, co-location, type of learning and critical roles
3. Project management – clarity of objectives, work breakdown, roles, management by exception
4. Senior management – setting strategy, sponsorship, providing resources and decision-making
5. Infrastructure – includes resources, equipment, and support services outside the programme
6. Organisational culture – extent of risk taking, willingness of others to extend extra effort, timeliness of decisions from others and informal communication channels

Table 10 presents the top five enablers, barriers and recommendations from the study's findings. Whilst the study only looked at one small part of HP's R&D operations, they do offer some insight into how to optimise innovation management, which may be relevant to other organisations involved in R&D.

Top enablers	Recommendations
1) Skilled people	Stress the importance of individuals to increase their skills and recruit new staff for new technologies where there is no in-house candidates
2) People are helpful	Promote and reward a culture of helping and sharing, particularly for new programmes. Actively create and support networks within the organisation
3) Management support	Ensure strong management support for all programmes, particularly fundamental ones
4) People working together	Create teams with a wide breadth of skills
5) Checkpoints provide focus	Use checkpoints to drive focus and decision-making. Communicate checkpoint decisions widely

Top barriers	Recommendations
1) Not enough resources	Conduct bottleneck analysis, using cross-functional teams. Ensure programme is flexible to respond to new market and technology information. Migrate organisation to allow faster deployment of resources
2) Hard to run experiments on production equipment	Invest early in new required equipment for exploratory research, avoiding bureaucracy for experiments. Transition the workforce and culture for flexibility and ambiguity
3) Lacking process capable equipment	Invest in flexible research tools and invest early in new tools for new fundamental programmes
4) Market planning	Develop ability to quickly identify marketing resources, strategy, and value proposition on innovations that are new to the company or to the world
5) Multi-site project	Establish strong communication links and develop clear roles and responsibilities

Table 10: Innovation process enablers and barriers, modified from Rivas and Gobeli (2005)

Following an analytical process of pattern matching from the study's interview data, presents the linkages between R&D programme attributes, and the frequency with which respondents reported enablers and barriers. The dimensions in Figure 20 allows the organisation to consider its project portfolio in the context of market and technology newness, and evaluates how best to accelerate innovation.

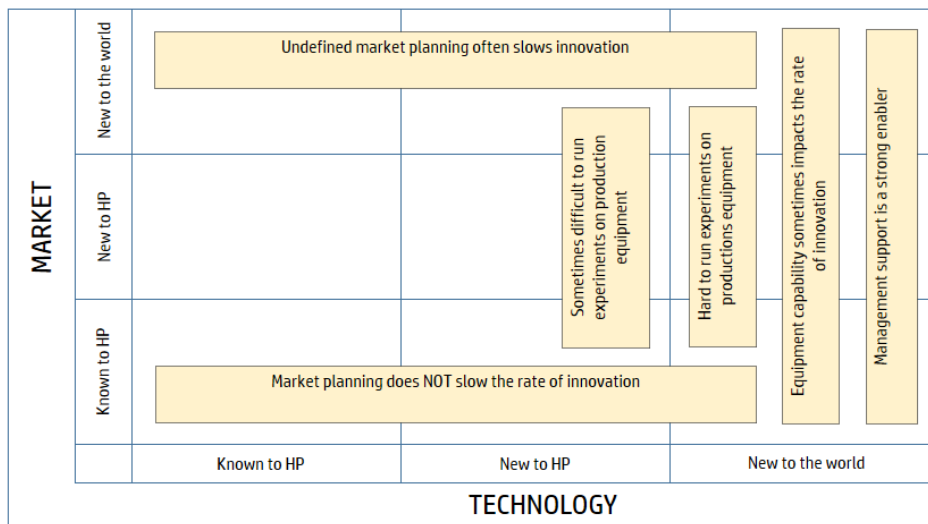


Figure 20: Market vs. technology newness, adapted from Rivas and Gobeli (2005)⁴²

As discussed above there is a distinction between 'research' and 'innovation', which has implications around the kind of teams, structures, budgets, timescales, and processes involved. Understanding this dimension can help prevent R&D failures by ensuring projects have the right resources in place.

New to world 'markets' is blue ocean territory which offers high rewards yet high risk, particularly for new to HP and new to world 'technology'. For incumbent ICT businesses such as HP not everything is developed in-house. Promising or proven technologies that are new to HP can be acquired. When combined with HP resources such acquisitions can open up new opportunities in all three types of markets.

Finally, the article suggests that accelerating innovation is closely linked to the rate of learning, which comes back to human talent. In knowledge intensive industries, it is suggested that the rate at which individuals learn is a critical source of sustainable competitive advantage.

5.4.6 Research and Innovation at SAP

The IT business is currently undergoing a major transformation determined by the potential of novel provisioning and consumption models for software: instead of each customer owning their applications and systems (the "on premise" model), consuming software as a service over shared computing and communication infrastructures (the "cloud" model) offers advantages in terms of an overall reduction of the total cost of ownership and scalability to actual and changing demands.

SAP has recognised that technology innovation is key to drive and master this transformation. To maintain a leading position in a market that is characterised by emerging technologies and business models, continuous disruption, and changing customer demands it is, however, of utmost importance to establish agile innovation processes that allow for response to changes and new contexts and avoiding what is known as the "innovator's dilemma". The processes that are aiming at transforming research into innovation at SAP are therefore centred on customer needs (not necessarily equivalent to the requirements expressed by a customer) and aim at balancing technology push and market pull, based on continuous evaluation and flexibility. Design Thinking (<http://dschool.stanford.edu/>), balancing feasibility, viability and desirability, is the approach of choice that guides SAP's research activities as well as innovation processes.

To implement these principles, SAP's research is characterised by:

- A decentralised approach, where research teams are part of the line of business their research topics are targeting. For instance, SAP's product security research team is fully integrated in the SAP line of business that is responsible for product security, including security strategy, secure development lifecycle, security requirements, security response and related activities. This allows researchers to better evaluate the relevance of their research and interact with their business stakeholders as part of the daily routine, helping to target research towards exploitation and commercialisation. The decentralised approach is complemented by small central teams acting as trend scouts and regularly interacting with the research teams to encourage out-of-the-box thinking.

- Instruments for collecting customer feedback and working on customer use cases, which allow researchers and innovators to directly interact with customers to recognise their needs and challenges. Use cases allow us to assess the innovation potential of research results by exposing them to the challenges faced in practice, including performance, scalability, economic viability, and market response. Not meeting these challenges is among the major reasons for research failing to lead to innovation.
- Collaboration with academic and industrial partners, which allows joining forces in pre-competitive stages to extend the basis of knowledge and the scope of research, is recognising the increased importance of ecosystems in the ICT business. Collaborators mutually benefit from this approach, since it opens innovation paths for academic research as well as extends the accessible body of knowledge for industrial partners. A cornerstone of SAP's collaboration with academia is a PhD program which fuels creativity in the company, supports addressing long-term topics and provides incentives for young talents to explore their ideas in an industrial context.

5.4.7 Research and Innovation at Technikon

Company Overview: Technikon, a small and dedicated Austrian SME with a multinational team of 20+ Engineers and Researchers has been successfully providing research services for the European Industry since 1999. It has received several state awards for its innovation actions and social responsibility. It develops hardware-software entangled security anchors based on physically uncloneable functions, works on the definition of security requirements and models, supports the execution of innovation projects and provides a complete set of secure collaboration tools for large distributed research teams.

Innovation lane: Technikon's long-term customer relations with leading IT companies gave it prioritised access to early stages of technology developments. It has availed of the opportunities of more than 35 international security research projects and in doing so has established a recognised group of young security specialists.

The engagement of Technikon in collaborative RTD projects is governed by the following strategic involvements:

The participation in large Industrial driven European bottom up projects (e.g. ARTEMIS "Internet of Energy project") to further develop and sharpen their security services and to cross-correlate project developments with their business ideas. This is the place for the creation of technology driven business and the identification of new opportunities.

The engagement in Medium or large scale research projects (e.g. FP7 Hint "Holistic Approaches for Integrity of ICT-Systems" provides for early bird access to emerging technologies and points Technikon towards novel, free-spirited solutions. This is the main place for the development of the Technikon knowledge base and the acceleration of employee engineering competence.

Small scale national research projects are used mainly to work on core technology and to create native intellectual properties (patents). There Technikon has the freedom to select the academic partners; who come up with their own contributions and therefore define the rules for exploitation rights.

These three involvement tracks have been proven as being a successful precursor for profitable industrial projects. This hands-on strategy is complemented by methodical measures and activities.

Innovation method: Technikon are a small company whose innovation method is applied correspondingly. Their approach to innovation involves the whole workforce without exception. Together they challenge and redirect their strategy twice a year. Innovation activities are assessed both internally and externally.

Feedback from customers is directly funnelled into the process. The business is fully client-centred with room for innovation set aside. Responsibilities are defined and internal activities are complemented with external experts. Technikon cooperates heavily with universities, they identify and safeguard novel IP and look for new methods.

Innovation rating: In 2014 Technikon took part in an external innovation assessment process. They have been rated for their innovation ability on the scale from 1 to 6 by the regional Economic Promotion Fund (KWF) against 23 other SMEs in terms of general conditions, corporate culture, knowledge & ideas, and structures & methods. They have been rated in all categories above the mean values. The results are shown in the Figure 21.

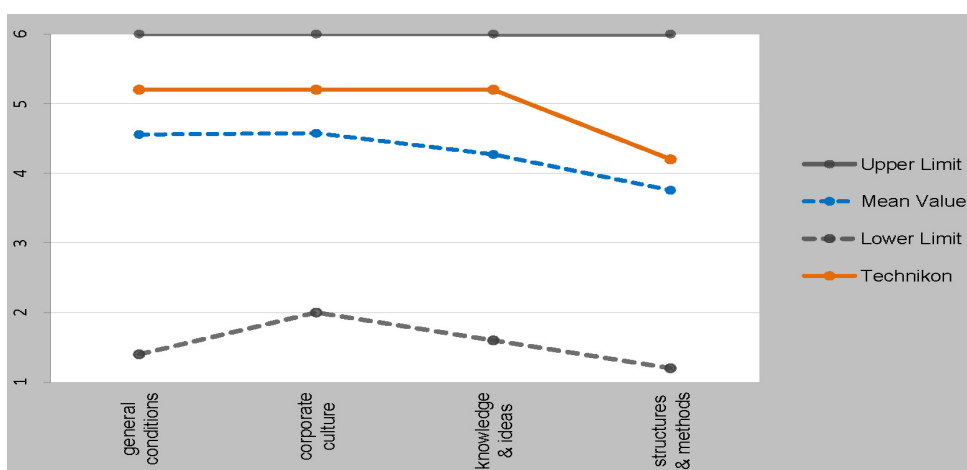


Figure 21: KWF SME Innovation Assessment

5.4.8 Research and Innovation with Industry Clusters – example LSEC – Leaders In Security

LSEC is a Belgian based not for profit association active throughout Europe. As ICT Security cluster LSEC is a network organization with members from enterprise end users, ICT security professionals, hard- and software vendors, network and system integrators, advisory services organisations, research institutes and other sector clusters. Founded in 2012 by KU Leuven together with seven ICT Security related companies, the organization grew to 135 active expert ICT Security members and over 6500 individual members active in various enterprise and government organizations.

LSEC is a proactive innovator, stimulating strategic process and technology innovation with IT security. We provide thought leadership amongst end user organizations and facilitate the transition to more secure and privacy consent products and services. LSEC bridges the gap between research and industry,

amongst other by providing innovation guidance and facilitate market entry to ICT security innovators, including cybersecurity, cloud and 'SaaSification', mobile and smart systems based upon sensors, IoT and wearables. LSEC coordinates innovation development between industries, while validating state of the art, and looking beyond.

The ICT Security Cluster works closely with both executives from the ICT security industry (CTO, CEO, Innovation Management) discussing interest in innovation, expanding products and services, approaching new markets and M&A activities. In some cases, there is an operational relationship with the innovation team or the incubator facilities. The association works equally close with the research departments focused on ICT security technologies, getting together frequently with the heads of the research departments and the individual researchers.

5.4.8.1 Innovation Pull Through: Working with Research Institutes to an involved validation and exploitation

The human effort on connecting the dots between ICT security industry requirements and the ICT research department can be partially automated, by continuously updating databases and / or aligning via social network activities; but is usually a human effort. Both are supported by the ICT Security cluster through a series of programs:

1. **Continuous evaluation and improvement:** An initial search on potential interests of the research activities, is supported by a continuous search for other industries, verticals and applications. Potential interests are continuously recorded and mined, with supportive means and measures. This requires a wide contact basis with end users and various industries from a neutral – non-commercial - perspective, typically a limitation of both research and industry. By actively involving those interests from initial and additional interests, they will be continuously informed and supported, allowing for a more active role in the project, and endorsing the interest; with proactive developments (proof of concepts) and adapted market research and analysis. This way innovation can mature on both ends.
- **Planning and developing exploitation:** Like any other product or service, innovations and research results also need some marketing. Marketing the research goes beyond the typical development of posters and research flyers. Industry and corporations need to get a first perspective on market potential, strategic value and differentiators. It includes the development of project and product websites, going beyond the listing the academic publications, dissemination of the research reports and includes scenario building or additional visualisations for specific industries. Specific market surveys can be undertaken, to allow for early on indications of potential interest by existing customers of some of the industry actors, without interfering with the ongoing business activities.

5.4.8.2 Strategic Innovation through Business Support Services:

The ICT Security Association supports its industry ICT Security Members by providing services supporting their innovation developments. By proactively approaching members with identified market challenges and needs, business requirements, research results and open innovation oriented industrial collaborative

projects; the cluster becomes a challenger and an innovation driver. The cluster will be capable in providing insights in strategic innovation indicating potential market disruptions from other domains effecting ICT security developments, and guiding to market potential in other markets or regions.

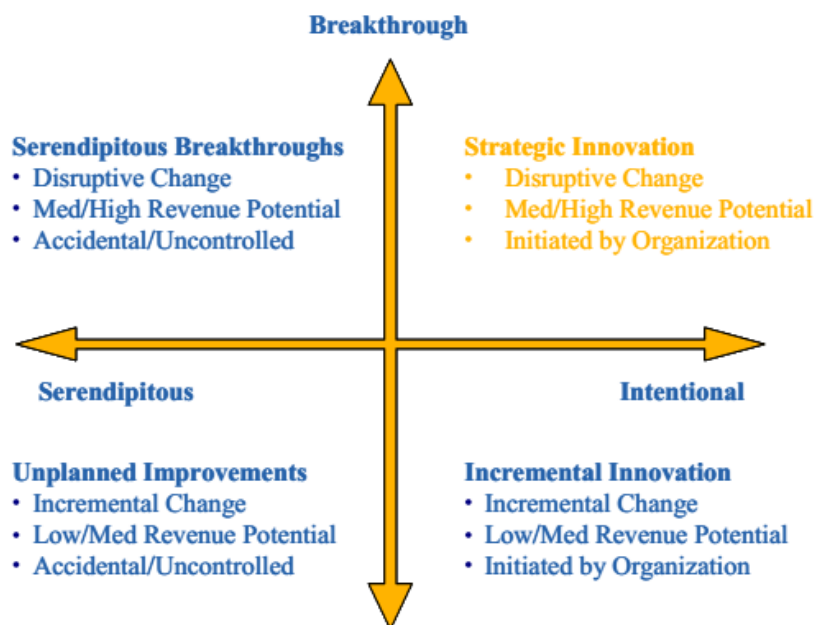


Figure 22: Source : Kaplan & Palmer, A Framework for Strategic Innovation - Innovation Point

LSEC provides collective and individual guidance & support, by:

1. being a sounding board for new ideas and developments,
2. yielding out new products and services with friendly customers from a neutral perspective,
3. providing insights into sleeping patents in research labs,
4. exploiting existing technology building blocks from research labs,
5. creating additional value from SME's technological innovations without clients or
6. SME's technological capabilities,
7. market monitoring and / or
8. shared procurement.

The ICT Cluster organisation is providing a number of business services to their SME members to facilitate access to markets, access to finance, technology transfer etc. and increasingly positioning itself as key agent for promoting re-industrialisation of its region and single point of contact for the ICT security industry. For that, specific services have been developed to foster for instance cross-sectoral cooperation (with Finance, Energy, Healthcare, Government, Retail, Process Industry, Automation), spot new business and R&D opportunities for its members and develop the necessary skills to successfully respond to such challenges. Identifying, guiding and coordinating the innovation process with, and for its Members has become a core service of the association.

5.4.8.3 Innovation based upon collaborative R&D projects

LSEC coordinates the development, or participation in various industrial collaborative innovation projects. On a regular basis, the association calls its constituency for potential joint interests, it communicates about joint demands, develops a specific topic on the basis of end user demand or identified market opportunities and gaps.

The association supports Research & Development driven growth, creates and enhances capabilities, provides for platforms to facilitate the take-up of R&D policy to attract more traditional SME's or to support industrial competitiveness. The cluster will address directly SME's and large industrial groups with identified needs and growth opportunities, stimulating cooperation together with other private actors and facilitating public actors participation. It seeks for synergies amongst the various stakeholders in order to be coherent with its cluster foundation. Specific educational and training activities can lead to the insight and development of a new joint approach, supported by a group of Members.

5.4.8.4 Leading Disruptive Innovation and Bridging market gaps

In some specific cases, the ICT Security association will take on the role to initiate an innovation development itself by deploying industry-wide international standards and certifications. By such a selection, it drives the industry to follow a specific direction on a certain topic or region. The association has also been initiating trial and pre-production deployments from pre-commercial developments or research technologies. By means of early market field-testing and by supporting disruptive technologies in proof of concept deployments, the cluster will lead to route to commercial take-up. This type of innovation allows for deployments of technologies with for instance a societal impact, and a reduced or slowed down commercial impact. The cluster can also decide to innovate with new products and services themselves, for instance when it considers the market not yet ready for broad commercial launches. This could happen when policy makers, public opinion or others support the sense of urgency of bringing innovation to market. It could also happen to support the initial market launch from an independent and neutral perspective, rather than from a specific business or company interest.

5.5 Initial Research & Innovation Analysis

This section has gone beyond academic discussions pertaining to research and innovation and attempted to discover real world applied examples of how innovation is facilitated and managed. It is clear from the case studies that many of the organisations utilise engagement at EU funding programmes as part of their overall research and innovation strategy. They also engage with Academia to pursue national initiatives while some organisations put an emphasis on their own staff for idea generation and innovation in a clear bottom-up approach. It is clear that an innovation strategy is an established part of their business development and that it is continuously revised in line with senior management and a top-down validation and prioritisation of activities. The next sections focus on the alignment of the theoretical innovation models presented in section 5.3 the case studies presented in section 5.4 and support initiatives presented in A.3 driving our final recommendations for future research and support in the cybersecurity market.

5.6 Economic analysis and the focus on incentives

In order to gain a more holistic picture of cybersecurity and privacy problems as well as the incentive structures to which actors are subject, it is necessary to apply economic principles to the interaction of actors. Economics enables the strategic analysis of security and privacy problems.⁴³

Many market problems that have been identified long ago in the Economics discipline resurface in cyber-security and personal data markets, sometimes in even more extreme forms.

Principles of economics can be applied to a problem, if some basic conditions apply: there need to be actors that employ strategies or plans to achieve a certain goal. Typically, the actors want to maximize their payoff by minimizing the effort invested to achieve the goal. In a nutshell, the Economics of Cyber-security and Privacy models IT security and privacy as decisions by the players involved. One of the challenges that the IPaCSO project is working toward is how to incentivize greater cyber-security and privacy, where market incentives seem to be insufficient for reasons of market failures due to problems such as information asymmetries.

The economics of cybersecurity applies principles of economics to the analysis of cybersecurity problems. The analysis is devoted to cost-benefit trade-offs faced by different market participants, their strategic behaviour and market outcomes (i.e. welfare effects). Cybersecurity analyses include not only firms and consumers, but also government or third-party players such as adversaries (hackers, etc.). Moreover, it is also possible to better understand the failure of successful innovation by market players, especially where the rents from innovation cannot be fully privatized (by the developer in the firm / the firm employing the developer or both).

The Economics of Personal Privacy research focuses on the application of economic analysis to personal privacy. Privacy is *personal* if it is *related to an identifiable individual* that can be singled out from an anonymous mass (Jentzsch et al. 2012)⁴⁴. Therefore, it focuses on incentives and actions of firms and consumers with respect to personal data. At the core of the analysis are privacy risks (or ambiguity)⁴⁵ and the ambivalent welfare effects arising from disclosure of personal data. Privacy economics focuses on the cost-benefit trade-offs of actors, their

⁴³ The following paragraphs are taken from Jentzsch, N. (2014b). State-of-the-art of the Economics of Cyber-security and Privacy, IPACSO Deliverable D4.1, *manuscript under review*.

⁴⁴ Jentzsch, N., Preibusch, S. & Harasser, A. (2012). Study on monetizing privacy – An Economic model for pricing personal information. Report for the European Network and Information Security Agency. Retrieved from: <http://www.enisa.europa.eu/act/it/library/deliverables/monetising-privacy>

⁴⁵ In the economics terminology, the term 'risk' describes situations of uncertainty with **known probabilities**, whereas the term 'ambiguity' describes situations of uncertainty with **unknown probabilities**. In decision theory, there is a known cognitive bias in individual decision-makers that explains that persons prefer a situation with known probabilities (i.e. risk) over one with unknown probabilities (i.e. ambiguity).

strategic actions, market outcomes and market failures. Moreover, it also includes the evolution of the competition among firms that personalize products or services and/or prices, while facing privacy-sensitive consumers. The economic impacts of government regulations are analysed as well.⁴⁶

5.6.1 Introduction to Economic Incentives

Again the following sections are quoted from Jentzsch (2014)⁴⁷. An economic incentive is an inducement (motivation) that leads to an action or behaviour, which renders a (positive) payoff for the actor. Payoffs are outcomes of cost-benefit trade-offs, where a rational actor's goal is to maximize the payoff. The actor's preferences order the outcomes of different choices he is confronted with. A rational actor seeks the optimal choice by seeking payoff maximization. If incentives are not aligned, they lead to suboptimal choices.⁴⁸ If a payoff is positive, it is a reward that provides an incentive for a specific action or behaviour. If a payoff is negative, it is a penalty that acts as a disincentive.

In economics, utility functions model cost-benefit trade-offs and therefore represent the preferences of actors. The outcome of specific actions, however, may be uncertain. In this case, risk or ambiguity is introduced in the decision model.

Payoffs may be monetary, but can also involve other – psychological – costs and benefits. For example, if a computer system is compromised and the personal data stolen used to commit a financial crime, the damaged party suffers a monetary loss. However, if the security incident in addition is made public, the targeted firm also suffers a reputational loss in the market. Such reputational effects may severely impair (or not) trust that customers place in the firm's security procedures. Psychological effects may also arise on the part of the damaged individual and involve reputational damage, humiliation or other anxieties.⁴⁹

As stressed by Gordon, the main objective of cybersecurity investments is to reduce the risk of security breaches. However, a twin-goal might be the reduction in variability of potential losses from cybercrimes. The latter increases planning and budgetary stability for companies⁵⁰.

It is a notoriously difficult matter to estimate the cost and benefit components in the area of increased IT security and privacy. For example, in order to obtain an

⁴⁶ We use the term 'privacy' to describe a situation of asymmetric distribution of personal information among market participants (see Jentzsch et. al 2012).

⁴⁷ Jentzsch, N. (2014). Deliverable D4.1 State-of-the-art of the Economics of Cybersecurity and Privacy, Innovation Framework for Privacy And Cybersecurity Market Opportunities (IPACSO) FP7 Project,

⁴⁸ Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, 3(3–4): 103 - 117.

⁴⁹ These might arise if personal data (such as names, address, credit card numbers, etc.) are peddled on a data black market and a number of unidentified criminals have access to the information.

⁵⁰ Gordon, L.A. (2007). Incentives for Improving Cyber-security in the Private Sector: A Cost-Benefit Analysis, http://hsc-democrats.house.gov/SiteDocuments/2007103_1155020-22632.pdf

economic incentive for the adoption of a new IT security system, the firm facing this decision needs to know all of the costs and benefits involved in obtaining the system in order to make an optimal decision. For the latter, the benefits have to over-compensate the costs. Moreover, as firms act under budget constraints, the option of spending more funds on improving IT security competes with other options that might improve revenues such as spending more on marketing.⁵¹

To make matters worse, there are **direct and indirect costs of cybersecurity investments**. The direct costs accrue only to the firm making the decision to purchase the new IT system, they are privatized. However, the indirect costs accrue to other market parties, who are not part of the decision-making in the firm. Consider the following example: The aggregated security in today's networked IT systems depends on decisions of all relevant market players in the system. The decision by a payment platform firm to purchase a more secure IT system influences the security of the whole value chain in online banking. The positive externalities can often not be fully internalized by the investing firm, leading to sub-optimal incentives to invest. Not being fully liable for insecure software impairs on processes of higher due diligence by software firms.

Externalities might also impact on consumers' utility. For example, a more insecure system might leave consumers with the damage of cleaning up identity theft issues showing up on their accounts, whereas a more secure system reduces these costs.

5.6.2 Conclusion

The market environment and competitive pressures in cybersecurity and privacy markets influence the strategic decisions of firms to invest in innovation. In order to understand these decisions better and what increases or decreases investment incentives, the operational environment needs to be understood first. Players who do not understand the environment they operate in are very likely to channel resources into innovations that have a higher likelihood of failure. Moreover, policymakers who do not understand the horizontal and vertical relations that exist, cannot improve the environment through a directed industrial policy (if that is a policy goal). At this stage, this type of analysis is limited by the lack of analytical tools and robust data.

First and foremost H2020 ought to strengthen analytical and information collection/production that enables an identification of cybersecurity markets as well as markets for personal data and privacy products and services. These tools ought to help to identify the main players as well as fringe players to gain insights into the competitive forces that also shape innovation processes in the firms. Moreover, the analysis will likely shed some light on the weaknesses that currently exist in the European markets with respect to the development and production of these critical products and services.

⁵¹ It has been stressed in the literature that IT security investments have primarily a cost-savings character compared to other measures that improve revenues (Gordon 2007; ENISA 2012)

5.7 Recommendations to H2020 on innovation processes

In line with the Digital agenda objectives⁵² and the Cybersecurity strategy⁵⁴, one of the challenges in Europe is to transform research results into tangible business opportunities. Evidence suggests³² that European research results do not reach the market in the majority of cases⁵³. One of the main challenges is technology transfer.

The industrial organisations involved in research projects need to position their research strategy in line with their business strategy for products and services. This includes their overall approach and viability of integrating new research results in the existing portfolio, sales support, licensing and pricing strategy.

Technology transfer, also called Transfer of Technology (TOT), is the process of transferring skills, knowledge, technologies and methods of manufacturing to a wider range of users who can then further develop and exploit the technology into new products, processes, applications, materials or services.

The process to commercially exploit research varies widely. It can involve licensing agreements or setting up partnerships to share both the risks and rewards of bringing new technologies to market. Spin-outs (such as Sedicii described in Appendix E2) are also used when the host organisation does not have the necessary will, resources or skills to develop a new technology. It has been established that there are many pitfalls for the innovation industry and the reality is that getting an idea, no matter how great, from concept to the market is fraught with problems, with many businesses failing at the development phase.

Therefore, in order to recommend which innovation processes are more suitable for speeding up the innovation process it is crucial, as a first step to identify the innovation uptake model properties that allow for the successful transformation of research outcomes into new products or innovative services. Moreover, it is important to find best practices such as those described in section 5.4 that can demonstrate the validity of the adopted models.

A comprehensive strategy that fosters innovation is needed on all levels, from the pan-EU to individual countries and regions. Typically, innovation is not limited to the research and development activities managed by a single company, but rather it is the result of a process of collaboration between a diverse and growing network of stakeholders, institutions and users. In fact, transferring the result of research in a successful service or product requires many complex complementary actions at the level of the supply chain, including, for example, **financial planning**,

⁵² Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the regions 'A Digital Agenda for Europe' /* COM/2010/0245 f/2 */ cited 14th July 2014 [http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=CELEX:52010DC0245R\(01\)](http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=CELEX:52010DC0245R(01))

⁵³ Ján Figel', European Commissioner for Education, Training, Culture, and Multilingualism http://europa.eu/rapid/press-release_IP-06-201_en.htm

organisational change, training of the workforce, intellectual property management and **marketing**. Some of these approaches are adopted by the EIT institute as described in Appendix C, as well as by its Knowledge Innovation Communities (KIC) of which one, EIT ICT labs, describes their evolving example of an innovation accelerator for ICT. There are more examples of organisations (public and/or private) implementing innovation policies that will be mentioned subsequently in this report. The following sub-section gives further examples.

5.7.1 Keys to speed up the process and success

EU Funded Projects should execute market studies for their research technologies defining business models this may enhance possibilities of project results to become economically viable.

1. Leverage experience from innovations centres specialised in innovation processes: As previously mentioned, in Europe, one of the most representative and recent examples of this type of centres is the KIC “EIT ICT Labs” with its network of nodes (linked centres of excellence where business, research and knowledge come together) spread across a growing number of states.

Obviously, several other examples already exist, at both single country or region level, where, with their own peculiarities, they all aim to bring innovation to the market. Anyhow, all the mentioned examples, although in different ways and each one with different levels of adherence according to its own governance, adopt a minimal set of high level general requirements, identified and summarized as following:

- Multi-stakeholder approach: This aspect is the fostering of fruitful collaborations between large industries and academia, involving SMEs, R&D organizations and policy makers. This is also the approach recommended by the New EU Cybersecurity Strategy⁵⁴
- Targeted focus: Every innovation centre should concentrate their effort and energy in the areas of interest they find more important, knowing that societal needs are an essential element to improve the quality of life.
- Metrics: An old adage that is still accurate today, states that you cannot manage what you do not measure. Having this in mind is clear that innovation companies need to implement a KPIs policy which includes the following examples of measurements: number of innovations incubated, the number of start-ups launched and the number of knowledge transfers.

The following list contains some organisations across Europe that takes into account the mentioned requirements to improve the process of work. These are further described in Appendix A.3.

- Italy

⁵⁴<http://www.eeas.europa.eu/policies/eu-cyber-security/>

- Technological districts⁵⁵
 - National Technology Platforms⁵⁶
 - Spain
 - CDTI (Centre for the Development of Industrial Technology)
 - OTRI (Offices for the Transference of Research Results)
 - UK
 - Technology Strategy Board⁵⁷
 - Catapult centres/ Technology & Innovation Centres⁵⁸
 - Center for Process Innovation (CPI) BAE Systems I3 Programme⁵⁹
 - Malvern Cybersecurity Cluster⁶⁰
 - The UK Innovation Forum⁶¹
2. A dedicated innovation team: innovation cannot happen in the performance engine of the company, so it is necessary to have a team dedicated just to innovation. It does not mean that the team has to be isolated from the rest of the company; to the contrary it has to leverage some of the assets and capabilities of the performance engine. Innovation is unpredictable and its risks cannot be measured with the same standards.
 3. Assets are very important: assets that a company uses to reach its objectives must be used to bring innovation to market such as customer relationships or an existing delivery model. Innovation is new and unpredictable but it can be aligned with the rest of the company. It is important to rely on what already works but not to the point of making it vulnerable, so the innovation team should be able to use resources and assets from the performance engine within a reasonable limit.
 4. Communication within the company: the connection between the performance engine and the innovation team has to be constant and well managed. Having the right leader in the innovation team is important to keep this link. The high level status of the company should be aware of both parts and avoid any possible conflict.
 5. Few innovations at a time: every time a company decides to innovate and therefore dedicate a team is like starting a new start-up company, which is a major organizational undertaking and nobody has the bandwidth to start hundreds of innovation initiatives.

5.7.2 Improving prospects of success

Actions to promote innovative technologies need to be cross-cutting, and specifically the uptake innovation activities will be more successful if they are cross-

⁵⁵ <http://www.distretti-tecnologici.it/>

⁵⁶ <http://www.unibo.it/NR/rdonlyres/1D7CB070-E635-4536-8B6C-5BD249CDE742/79383/MUccellatore.pdf>

⁵⁷ <https://www.gov.uk/government/organisations/technology-strategy-board>

⁵⁸ <https://www.catapult.org.uk/>

⁵⁹ www.baesystems.com

⁶⁰ <http://www.malvern-cybersecurity.com/>

⁶¹ <http://uk-if.org/>

country, cross-sector; cross-organisational, or cross-technological as EIT ICT labs has experimented.

We can expect that the EIT-ICT Labs process will also show that collaborative actions of multiple organisations involved in the same innovative project can achieve more than the activities of a single organisation, benefiting from the increased expertise created by joining forces and optimising the use of resources brought in by different organisations. This already mentioned important aspect was further fostered by EIT introducing in the Call for Activities 2015 a new type of activity named “High Impact Initiative Activity”. To create a very effective and dynamic collaboration environment with critical mass, all of the work on each HII Activity will take place in the relevant Co-location Centres. This means that partners need to commit to facilitate this by enabling their participating team members to work at one of the participating Co-location Centres.

Trends in ICT technology also demonstrate that **technologies from different areas can be complementary**, and can boost innovation achievements. For example, the rapid evolution of the Internet of Things domain is also enhanced by the Big Data domain, because fast processing of huge volumes of context data enables competitive advantage. Similarly, it is often the case that different industry sectors use the same innovative technology (e.g., robotic technologies are used today in a variety of sectors). Therefore, it is very beneficial for the society, but also for the innovation technology producers, if innovations involved in a transfer to market process are cross-sector.

Previous recommendations by the CSA SecCord⁶² in analysing the impact of EU funded Trust and Security projects provides relevant insight into these challenges and should be considered within this initiative. The strategic directions include EU citizen security, Security of EU SMEs, EU economy and product development. In addition they provide some analysis on whether the funded projects met the work programme goals and identified gaps such as:

- scalability challenges
- protocols for privacy infrastructure of multi-identities
- advancement of privacy in hardware levels

Further work within this deliverable aims to leverage previous analysis and clustering initiatives to evaluate the challenges that are present in the area of technology transfer and economic impact and exploitation.

5.7.3 Best practice

Successful innovators can follow the model of the EIT ICT Labs even without being directly supported specifically by this organization. This is the example of SecurityMatters⁶², a company that has followed this model and is now a recognized supplier for cybersecurity technologies for critical infrastructures.

SecurityMatters is a spin-off of the Security groups at the Technical University of Eindhoven and Technical University of Twente (the Netherlands). It develops and deploys intrusion detection systems encompassing network monitoring, intelligence and protection technology. SecurityMatters has developed a new approach to

⁶² <http://www.securitymatters.com/>

securing computer networks, called self-configuring deep protocol network whitelisting, which was the result of research carried out by the Security group in the domain of network intrusion detection. This work initially resulted in scientific publications accepted at top-level conferences and journals (such as USENIX LISA, RAID, Journal of Network Management, etc.). Parts of this work were also developed further in a number of national and international R&D projects.

After the initial proof-of-concept prototypes were developed, the founders of SecurityMatters applied for and received in 2009 a “Dutch Phase II Valorisation grant”⁶³ (a funding instrument valorisation grant for entrepreneurial researchers) to start the company. Within this grant framework they also created a consortium of Dutch companies to apply cybersecurity technology to national critical infrastructure. Throughout 2009-2011 the company executed 3 pilots with Dutch companies and evaluated its product called SilentDefence. Successful completion of these pilots led to recognition of the SilentDefence toolset. Recently the company won a contract with Boeing⁶⁴, and has become a worldwide-recognized producer of network monitoring and intrusion detection systems with offices in the Netherlands and the US. The success story of the SecurityMatters start-up is evidence that the EIT ICT Labs approach to foster innovation works in practice, even if the company itself was not incubated by this organization. Yet the focus on the **alloy of research results and industry needs**, and the **support offered by the Dutch government** to launch the start-up and execute pilots, allowed the company to achieve commercial success.

⁶³ <http://www.stw.nl/Programmas/ValorisationGrant/>

⁶⁴ <http://www.utwente.nl/en/newsevents/2014/2/286688/ut-spin-off-securitymatters-new-supplier-for-boeing>

6 Summary of recommendations

The recommendations of this report go toward maximising the beneficial impact on European economy and society of NIS Research and Innovation (R&I). It is widely perceived that malicious threat agents have the upper hand over the NIS community. The press is full of articles on newly-discovered vulnerabilities and of security breaches causing significant financial losses and damaging reputation. Moreover, concerns about how to deploy potentially-valuable new technologies without increasing risk unacceptably are delaying their adoption.

Our aim as NIS professionals must be to escape from a situation of perpetual firefighting and gain the initiative over the threat agents. Achieving such a change represents a significant challenge, but doing so will yield collective benefits in terms of economic stimulation and reduced crime protecting vulnerable citizens. An effective European NIS industry sector will also be an economic powerhouse and major employer in its own right. A comprehensive strategy that fosters innovation in cybersecurity is needed on all levels, from the pan-EU to individual countries and regions.

In the short term, considerable benefits can be realised by spreading awareness of NIS issues, establishing minimum NIS hygiene standards, best practice guides, criteria and standards to support secure solution procurement and gradually bringing all organisations up to the standards of the best (taking into account their different circumstance). Regulatory and institutional initiatives such as the NIS Directive, forums and infrastructure for sharing threat intelligence also offer the prospect of significant collective benefit. Such issues are the domain of WG1 and WG2, however, in WG3, we must focus on achieving impact through R&I, i.e. by advancing the state of the NIS art.

Research and Innovation are distinct processes, often carried out by different communities. Research addresses relatively fundamental challenges that require sustained and dedicated effort over an extended period. Innovation, however, must be agile in order to bring potential solutions to market in advance of competitors. Both are high-risk activities offering low probability of success, but potentially large returns. The next sections summarise the key recommendations.

6.1 Input to the NIS Strategic Research Agenda

Europe has an excellent reputation for original research that extends to areas that are highly relevant to NIS, but is perceived as less good at turning research results into successful products and businesses. But is it actually the case that other economies are reaping the benefits for Europe's investment in NIS-related research? We have not been able to answer this question from readily available sources. It is clear that some initiatives started in the EU have then been acquired by other regions and this in itself is often a financial success story for the organisation involved but it is migrating the innovation. Currently, NIS requirements are dictated by the need to react to evolving types and increasing sophistication of threats, and to innovations in the technical, business and societal context. How these external factors will change is very difficult to predict.

We recommend commissioning a study that:

- *Traces the research origins of concepts underpinning successful NIS products and services;*
- *Tracks whether and how past NIS research results have been exploited, especially those perceived as significant at the time the research was performed;*
- *Devises success indicators for applicable NIS research results and sets up a system for monitoring the future exploitation of results.*

To establish a stable and consistent research agenda, we need to get ahead of the game and focus on principles required to underpin the vision of a secure society. The most fundamental requirement is the creation of an engineering science of secure/trustworthy software and human-technical systems, including reference architectures and design patterns, so that security can be built into systems from the beginning.

NIS is applicable to systems on all scales and support composition and decomposition of systems. It needs to take into account complex dynamic aspects including the interaction of security operations and governance processes with on-going business activities and the actions of communities of threat agents. It must also provide the means of balancing the rights and responsibilities of all stakeholders and effective mechanisms to assert rights and enforce transparency and accountability. It should also take into account the need to enable and encourage an effective and competitive market in NIS products and services, by ensuring that barriers to innovation are low.

The research agenda must be owned by a coalition representing all stakeholders, including end-user organisations and NIS vendors and service providers as well as public authorities and citizen rights organisations. It must be managed actively, and revised whenever necessary. Furthermore there must be means of tracking progress towards its goals.

To provide security, an organisation's defences must form a coherent set of capabilities that co-operate harmoniously. The difficulty in predicting future NIS requirements and the liability for those requirements to change rapidly, mean that evolvability of service is a key attribute. There is a clear need for a holistic, systems approach to security, and hence for a set of compatible and interoperating security capabilities.

The NIS research and innovation portfolio should include projects that are aimed at defining and maintaining reference architectures, frameworks and interface standards, and encourage and co-ordinate the creation of ecosystems of compatible and interoperable products and services across a cluster of research and innovation projects. It is important that these architectures, frameworks and standards are defined in such a way as to promote competitive innovation, and are designed for evolution.

This further suggests an approach to NIS solutions in which mix-and-match security capabilities are deployed on standards-based platforms. Creating appropriate platforms is a challenge in its own right.

The NIS research and innovation portfolio should include projects that are aimed at providing innovation-friendly NIS platforms, i.e. technological environments in which a range of novel NIS products and services can be brought to market or deployed in combination to protection applications and processes.

This will also encourage the establishment of a competitive European NIS market place, by lowering the barriers to entry to new players. There will be opportunities for providers of best of breed platforms and individual services as well for providers of complete solutions.

We have proposed (in Section 4) a requirement-driven methodology designed to contribute to an NIS research roadmap that will prioritise the research topics with the highest potential for market impact. The idea is that we will end up with a list of research goals that can be justified (at least in part) because they are derived from (and can be traced back to) high-priority security requirements that are currently not met. The logic of the methodology leads from stakeholder concerns, to use cases that make those concerns concrete in specific scenarios, to capabilities/services that would address those concerns, from which we can define research goals by generalisation or identifying enabling advances.

Note that ideally there would be a many-many relationship between scenarios and research goals, and research goals that affect multiple scenarios will be ranked higher in terms of impact. The basic approach starts with identification of a range of challenging future scenarios drawn from different industries. Use cases within those scenarios are then defined and analysed (from different stakeholder viewpoints). The analysis leads to abstract descriptions of collections of services required to satisfy the stakeholder requirements. The next step is to generalise across scenarios to obtain generic security capability sets from the collections of services.

The capabilities for which enabling technologies are currently missing are the basis for defining research goals, which can then be prioritised according to the number and economic/societal value of their contributions to use cases/scenarios. To obtain realistic timeline for the roadmap, the likely timescales and success probabilities for achieving the research goals also needs to be taken into account.

We believe there is merit in the requirement-driven road-mapping approach proposed in this report, but carrying out to the required depth it is beyond the scope of current WG3 activities. Furthermore, the roadmap would have to be revisited regularly and maintained actively.

6.2 Stimulating and promoting innovation

One of the challenges in Europe is to transform research results into tangible business opportunities. Evidence suggests³² that European research results do not

reach the market in the majority of cases⁶⁵ with technology transfer being one of the main challenges.

Therefore, it is crucial as a first step to identify the properties of the innovation uptake model that allow for the successful transformation of research outcomes into new products or innovative services. It is also important to find the best practices such as those described in section 5.4 that can demonstrate the validity of the adopted models.

A comprehensive strategy that fosters innovation is needed on all levels, from the pan-EU to individual countries and regions. Innovation is not typically limited to the research and development activities managed by a single company. It is the result of a process of collaboration between a diverse and growing network of stakeholders, institutions and users. Transferring the result of research in a successful service or product requires many complex complementary actions at the level of the supply chain.

6.2.1 Keys to speed up the process and success

Experiences from innovation centres should be leveraged. One of the most representative European examples of this type of centre is the KIC “EIT ICT Labs” with its network of nodes spread across a growing number of states (see Appendix C).

It is necessary for an organisation involved in innovation to have a dedicated innovation team which is distinct from the rest of the organisation. The innovation team should not be isolated from the rest of the company as it will need to leverage some of their assets and capabilities.

The separation of the innovation team is primarily that of a separation in terms of how their outputs are evaluated; innovation is unpredictable and its risks cannot be measured with the same standards as other departments.

Assets that a company uses to reach its objectives must be used to bring innovation to market. It is important to rely on what already works so the innovation team should be able to use resources and assets from the rest of the organisation.

The innovation pipeline should be managed so as to have constructive focus on a limited number of innovations at any given time. Doing this avoids the problems associated with having too many diverse projects.

Several other examples which aim to bring innovation to the market already exist. These examples adopt a minimal set of high level general requirements, identified and summarized as:

- Multi-stakeholder approach: This aspect is the fostering of fruitful collaborations between large industries and academia, involving SMEs, R&D organizations and policy makers. This is also the approach recommended by the New EU Cybersecurity Strategy⁶⁶

⁶⁵ Ján Figel', European Commissioner for Education, Training, Culture, and Multilingualism http://europa.eu/rapid/press-release_IP-06-201_en.htm

⁶⁶ <http://www.eeas.europa.eu/policies/eu-cyber-security/>

- Targeted focus: Every innovation centre should concentrate their effort and energy in specified areas of interest, knowing that societal needs are an essential element to improve the quality of life.
- Metrics: you cannot manage what you do not measure. With this in mind it is clear that innovation companies need to implement a KPIs policy which measures the number of innovations incubated, the number of start-ups launched and the number of knowledge transfers.

Appendix A.3. describes some organisations across Europe who have successfully utilised these requirements.

6.2.2 Improving prospects of success

Actions to promote innovative technologies need to be cross-cutting, and specifically the uptake of innovation activities will be more successful if they are cross-country, cross-sector; cross-organisational, or cross-technological.

The EIT-ICT Labs process demonstrates that the collaborative actions of multiple organisations involved in the same innovative project can achieve more than a single organisation. This is due to the fact of collaborative efforts benefiting from the increased expertise created by the optimisation of the pool of resources and competencies of the different organisations. Thus effective collaborative actions projects should be promoted in Horizon 2020.

6.3 Total NIS R&I

Knowledge generated in research projects is raw material that is processed by innovation projects to produce novel products and services, for example, to counter new threats, enable secure use of new technologies and business practices, respond to changing societal and regulatory pressures. Research projects are relatively long-lived, and the pace of advance of the scientific state of the art is generally slow, but punctuated by infrequent and unpredictable major breakthroughs and paradigm shifts. However, major research result can fuel many innovations in different application contexts.

It is straightforward to see how research influences innovation, though there is certainly scope for improving the efficiency of information/technology transfer both in terms of timeliness and completeness (i.e. ensuring all exploitable information reaches everyone able to exploit it). For example,

To encourage efficient technology transfer, and prepare the way for innovation, research projects should:

- *Include application case studies, demonstrators and pilots to guide projects, validate results, and establish an effective two-way dialogue with 'innovators' and demand-side stakeholders;*
- *Consider how the threat environment will respond to widespread knowledge of the new NIS technologies;*
- *Consider compatibility of the NIS technologies being developed with current tools and practices. Will market disruption be required for the technology to be exploited to its full potential?*

- *Include business-oriented activities such as exploitation roadmapping and preparation of outline business models and investment cases.*

NIS researchers should be provided with opportunities to train and gain practical experience in innovation and entrepreneurship. They should be encouraged to take their research results through to innovation by forming start-up companies and/or transferring to/within industry. Both academic and industrial carrier paths and qualifications should recognise the value of mixing research, innovation and operational experience.

It is also important to make it easy for entrepreneurs and innovators to discover applicable research results. Often, potentially valuable research results are generated before the enabling technologies and market conditions are right for them to be exploited. Too often, these are forgotten, and research is wastefully repeated or the advantage given to later-moving competitors.

A searchable repository of historic results, combined with an innovation broker services could help release the latent value of NIS research. Royalties or licensing fees could be paid to the owners of the results in return for making their results available to innovators.

Making the research process responsive to the needs of innovation and hence the market is a more difficult issue due the mismatch of timescales. This is a problem in many ICT-related disciplines, but is especially the case for NIS because the pace and direction change is driven by the accelerating arms race with an increasingly diverse set of threat agents including extremely sophisticated, well-funded and organised elements. Therefore,

NIS research projects should be structured and organised in such a way that the direction of research may be adapted during the life of projects as the market evolves.

The difficulty in predicting future NIS requirements and the liability for those requirements to change rapidly mean that it is important that future NIS platforms and the capabilities resident within them allow for a continuous and flexible evolution of services. Easy adaptability in the face of a changing operational environment is arguably more important than providing highly optimised support for a particular flavour of security service.

Similarly,

An agile approach to combined R&I and operations for NIS would be of great value. Such a 'Total NIS R&I' methodology could, for example, be based on the DevOps approach to integrated software development and operation, but specialised to NIS and extended 'upstream' to embrace aspects of R&I.

A Total NIS R&I approach would need to be supported by an experimental testbed platform in which research ideas could be explored in a realistic context alongside more mature 'innovation phase' and operational services using real data and realistic threats. This would also be a good way to way to acquire feedback from a

full range of stakeholders. The interdependence of NIS capabilities means that there are benefits to making such platforms open to support collaborative R&I as long as commercial confidentiality could be provided. Thus,

NIS research and innovation would be facilitated by the provision of shared experimental testbeds, avoiding wasteful duplication of effort and providing capabilities beyond the means of individual projects. These could include simulation of a range of application and threat scenarios. Cross-project experimental prototyping would be strongly encouraged. The testbed environments themselves could act as prototypes for innovation-friendly operational platforms.

Finally, the impact of NIS R&I depends on a complex set of interactions between available technology, societal pressures, perceived and actual threats, and market dynamics. For an innovation to be successful, it will have to displace incumbent products in a similar niche and work harmoniously with complementary products, or else disrupt the market bringing about a paradigm shift. Either way there are barriers and inertia to overcome. To develop a better understanding of these interactions,

We recommend research be performed to better understand the dynamics of NIS innovation and viewing the NIS market as a complex dynamic system, taking into account the goals and behaviours of legitimate stakeholders and of malicious actors

Appendix A Summaries of source documents

A.1 Pierre Audoin Report for the UK Department of Business, Innovation and Skills

The following summarises relevant aspects of the report, “Competitive Analysis of The UK Cybersecurity Sector”, which was compiled by Pierre Audoin for the UK Department of Business, Innovation and Skills (BIS). Although its focus is on the UK situation, many of the conclusions would apply to other European markets as well.

Motivation from a BIS perspective:

- Make the UK one of the most secure places in the world to do business in cyberspace, resilient to cyber-attack and better able to protect our interests, helping to shape an open, vibrant and stable cyberspace that supports open societies
- Build a successful and competitive knowledge-based industry to exploit the undoubted need for cybersecurity in the UK and other countries
- Allow citizens to conduct business, commerce and our private lives digitally, while in a safe environment

Threats to individual, corporate and government activities online come from three primary sources:

1. Criminal behaviour
2. Hacktivism
3. Espionage

There are a number of major IT trends that (together with the threats mentioned above) are challenging conventional approaches to IT security. Each of these trends is both dependent on cybersecurity innovation, and can itself play a role in improving the overall effectiveness of a secure environment:

1. Cloud computing
2. Mobility
3. Social computing
4. Big data & analytics
5. Rapid and continuing increase in the number of devices connected online
6. De-perimeterisation: the disappearance of clear boundaries between, networks, businesses, economies and aspects of the lives of individuals (work, family, leisure, ...).

Technical field that can contribute to new security solutions include:

1. New security architectures
2. Intelligence and Forensics
3. Cryptography (especially Quantum)
4. Artificial Intelligence
5. Behavioural Analytics (Network and Human)
6. Identity management
7. Biometrics

Hot topics in today's cybersecurity sector are:

1. Risk Management
2. Vulnerability Management
3. Asset Discovery and Management
4. Mobile Security
5. Critical Infrastructure/Industries/SCADA protection
6. Secure-by-design development
7. Governance systems
8. Security Operation Centres (SOC)
9. Management Security Services (MSS)

Four distinct sub-markets can be distinguished with different requirements and supply chains:

1. Defence and intelligence
2. Government, other than Defence & Intelligence
3. Enterprises
4. SME and consumers

The supplier community operating within the cybersecurity sector is both complex and fragmented. Major categories of supplier include:

- Global technology vendors and systems Integrators
- Defence contractors
- Local IT service specialists
- Domestic technology vendors
- Major Global consultancies
- Telecoms operators
- Global technology vendors
- Universities and administrations

A.2 CAPITAL - Cybersecurity research Agenda for Privacy and Technology challenges

CAPITAL is an FP7 collaborative project being carried out by members of the EOS (European Organisation for Security) consortium. Its main objective is to deliver an integrated research and innovation agenda for cybersecurity and privacy. CAPITAL Deliverable D2.1: List of Emerging Areas of Information Technology identifies key topics and items of future research in the realm of cybersecurity. It follows a bottom-up approach by which technological areas are classified according to their expected challenges and impact in cybersecurity and information privacy, and then it looks at how the application domains rely on these ICT areas for their progress. Another EOS project, CYSPA, takes a complementary approach, focusing on the subset of domains that make use of ICT technologies and analysing the impact of cyber disruptions as a result of the application of the latest advancements in IT in these domains.

The methodology which has been used by CAPITAL to select of the key emerging ICT areas follows the steps below:

1. Identification and study of existing relevant reports and literature sources, including recent ENISA threat reports, NIST reports, SANS Institute reports,

- yearly threat reports from various companies, and cybersecurity research agendas.
2. Conduct of a survey of internal experts within the CAPITAL partners which helped to draft the “key area profile” table included for each selected area.
 3. Identification of ICT areas where outstanding issues of security and privacy are most likely to be found.
 4. Filtering and selection of key, independent and complementary areas, in order to expand upon them and guide future work in CAPITAL

As a result of the above methodology 20 emerging areas have been listed but after the consortium partners’ contribution the list has been reduced to the 8 main emerging areas listed below:

1. Future Clouds
2. Future Security and Privacy Incident Management
3. Cybersecurity and Privacy Engineering
4. Internet of Things
5. Mobile Computing
6. Big Data
7. Critical Industrial Systems
8. Online Trust and Transparency for Privacy

These can be divided into two main categories:

- IT trends with implications for security and privacy (Future Clouds, Internet of Things, Mobile Computing, Big Data and Critical Industrial Systems)
- Emerging technical fields aimed at providing security (Future Security and Privacy Incident Management, Online Trust and Transparency for Privacy)

Comparing the above areas with the IT trends and the hot topics identified in the PAC study for BIS, we can see substantial consensus regarding the disruptive technologies. Regarding the two security technical fields identified by capital, the first is essentially about next-generation security information and event management (SIEM) systems, and is closely related to the Intelligence and Forensics field and Security Operations Centres topic from the BIS/PAC report. Regarding the second field, there is no obvious counterpart in the BIS/PAC report; it is possible that trust and privacy were regarded as out of scope.

A.3 Innovation organisations in EU member states

The following is a non-exhaustive summary of institutes or organisations dedicated to foster innovation among researchers, companies and SMEs in some states of Europe.

A.3.1 Italy

Technological districts⁵⁵: In Italy, there are currently about 25 technological districts formally approved by the Ministry of Research and the relevant local government; some of these districts focus on the development of ICT technologies and have a direct impact on the activities of the development of the Italian national capacity in the area of cybersecurity. The Technological Districts are therefore an organisational structure with great potential in increasing the technological level and

competitiveness of a specialised territorial supply chain; to establish a Technological District, the presence of different actors on the territory is needed:

- Universities or research centres, capable of providing scientific and technological knowledge, as well as highly specialised training, on the relevant area of specialisation
- Medium and large company capable of receiving and exploit such knowledge
- A network of small and medium-sized companies which, as a “technology partners” can become the bridge between universities and large companies
- An appropriate governance structure

National Technology Platforms⁵⁶: it is an organisational structure that promotes innovation through collaboration between government, the private and public research system, companies and end-users. It identifies scenarios of technological development of medium-and long-term thematic priorities, and identifies the means of implementation; it interfaces with similar experiences developed at EU and international levels, develops networking and coordination of national research actors, high-tech clusters and centres of excellence. Among the Italian Technology platforms, we can mention SERIT the one devoted to homeland security research that has a specific mission in cybersecurity. The main research topics identified by SERIT in cybersecurity for 2013 are:

- Cyber-physical protection systems;
- Cyber intelligence via information management;
- Design and development of crisis management systems;
- SCADA and Smart Grid Security;
- Cloud Computing Security;
- Mobile Security.

A.3.2 Spain

CDTI (Centre for the Development of Industrial Technology): it is a national Public Business Entity⁶⁷, answering to the Ministry of Economy and Competitiveness, which fosters the technological development and innovation of Spanish companies. It seeks to contribute to improving the technological level of the Spanish companies by means of implementing the following activities:

Financial and economic-technical assessment of R&D projects implemented by companies;

- Managing and fostering Spanish participation in international technological cooperation programmes;
- Fostering international business technology transfer and support services for technological innovation;
- Supporting the setting up and consolidating technological companies.

OTRI (Offices for the Transference of Research Results): Offices for Transference of Research Results⁶⁸ were created at the end of 1988 as structures

⁶⁷ <http://www.cdti.es/index.asp?idioma=1>

⁶⁸ <http://www.universidad.es/en/spain/research-spain/research/research-results-transfer-offices-otris>

for promoting and facilitating cooperation in the area of R&D activities between researchers and businesses, both in Spain and across Europe. The OTRI play a major role as part of the efforts made by the Spanish universities to bring their activities into line with society's needs. The general objectives of the OTRI are as follows:

- To promote the participation of universities community in R&D projects;
- To create the database of knowledge, infrastructures and R&D offer in the respective universities;
- To identify the results generated by the research categories, assess their transference potential and pass them on to companies, either directly, or in collaboration with other interfaces;
- To facilitate the transference of these results to the companies;
- To inform about the different R&D programmes, facilitating the technical aspects of project preparation and managing their processing.

ERAC Peer Review of the Spanish Research and Innovation System

A report⁶⁹ commissioned by the European Commission delivered by an Independent Expert Group for the Spanish Ministry of Economy and Competitiveness, the Spanish Secretary of State for Research, Development and Innovation and for the European Research Area and Innovation Committee.

A.3.3 UK

Technology Strategy Board⁵⁷: it is a non-departmental public body sponsored by the UK Government Department for Business, Innovation and Skills. Its aim is “to accelerate economic growth by stimulating and supporting business-led innovation”. To achieve this aim, the TSB has the following goals:

- To accelerate the journey between concept and commercialisation;
- To connect the innovation landscape, by building strategic relationships with other innovation players, creating a more effective innovation environment;
- To turn government action into business opportunity, by identifying how policy, standards, and regulation can stimulate innovation, and by encouraging government to act as ‘lead customer’ for businesses that can solve public sector challenges;
- To invest in priority areas based on potential, by focusing on thematic areas which are most likely to generate UK economic growth and which address global challenges and opportunities;
- To continuously improve its own capability, by developing its people and processes to be fast, flexible, and focused on business needs.

Catapult centres / Technology & Innovation Centres: Catapult centres⁷⁰ are initiatives led by the aforementioned TSB that aim to catalyse and support research and development, foster links between business and academia and promote economic growth. The UK has 7 catapult centres, each centred around a specific location and each focusing on a specific field of innovation. These include:

⁶⁹ http://www.mineco.gob.es/stfls/MICINN/Prensa/FICHEROS/2014/140801_final_report_public_version.pdf

⁷⁰ <https://www.catapult.org.uk>

- High-value manufacturing;
- Cell therapies;
- Off-shore renewable energy;
- Satellite applications;
- Connected digital economy;
- Future cities;
- Transport systems.

Centre for Process Innovation (CPI): it is a UK-based technology innovation centre [CPI] and part of the High Value Manufacturing Catapult. They use applied knowledge in science and engineering combined with state of the art facilities to enable their clients to develop, prove, prototype and scale up the next generation of products and processes.

BAE Systems I3 Programme: Investment In Innovation⁵⁹ is a multi-million pound investment programme run by BAE Systems, which supports SMEs and academia in accelerating the development of research and innovation. The focus of the programme is on technologies of relevance to the defence and security sector, with current areas of interest including cybersecurity, surveillance and biometrics. Available support includes funding, knowledge and skills sharing, provision of facilities and examples of governance and best practice.

Malvern Cybersecurity Cluster: Malvern Cluster⁶⁰ is a group of 50 SMEs located in Malvern, Worcestershire, who collaborate on a range of initiatives to build their businesses and help local organisations to improve their cybersecurity. The Cluster provides a variety of services to its members and the local community including:

- Regular meetings for members, including core SME members and broader engagement with larger organisations;
- Skills and training initiatives including visiting local secondary schools and supporting development of apprentice programmes;
- Events for the general public to increase awareness of cybersecurity risks and mitigations.

The UK Innovation Forum (UKIF): The UK Innovation Forum⁶¹ was established with the support of the Science and Technology Facilities Council, a non-departmental public body within the UK, and aims to support collaboration between businesses, investors, research and academia. To achieve this, UKIF provides a number of services to organisations both in the UK and overseas:

- Online forums to support collaboration and provide a mechanism for finding innovation partners;
- A job board for opportunities within UKIF member organisations;
- Regional and national meetings and conferences;
- A database and newsfeeds of licensable technologies from UKIF members.

Appendix B model

United States example of R&D Execution

The following is a summary of Maughan et al. (2013) describing an R&D execution model based on experience from cybersecurity programmes in US R&D funding agencies. It is intended to increase significantly the success rate of the transition of projects from the research community to engineering development. While the model was developed by the cybersecurity R&D program at the United States Department of Homeland Security Science and Technology Directorate, it is generally applicable to other R&D organisations.

Reasons why there is a gap between cybersecurity research and engineering development:

1. Difference between the personality types and skills needed for research and business
2. Lack of financial incentives and sufficient motivations for researchers to pursue commercialisation of their results

Complexities in the research, development and transition process

1. Differences in the goals, timeframes, and funding levels of the different players in the process (researchers, industry and operational users)
2. Gaps in staff expertise, lack of funding and flexibility in negotiating agreements with outside parties

Key factors that will help to improve the success rate of technology transition:

1. Active collaboration among researchers, industry and operational users during all phases of technology transition
2. Need to share experiences, working models and best practises for technology transition in the cybersecurity R&D community
3. The existence of a key requirement and evaluation criterion
4. Transition must be designed into the programme from its first inception
5. Engage customers before, during and after the research
6. Granted support from the funding agency to the researchers which will help be informed for market up to date technology

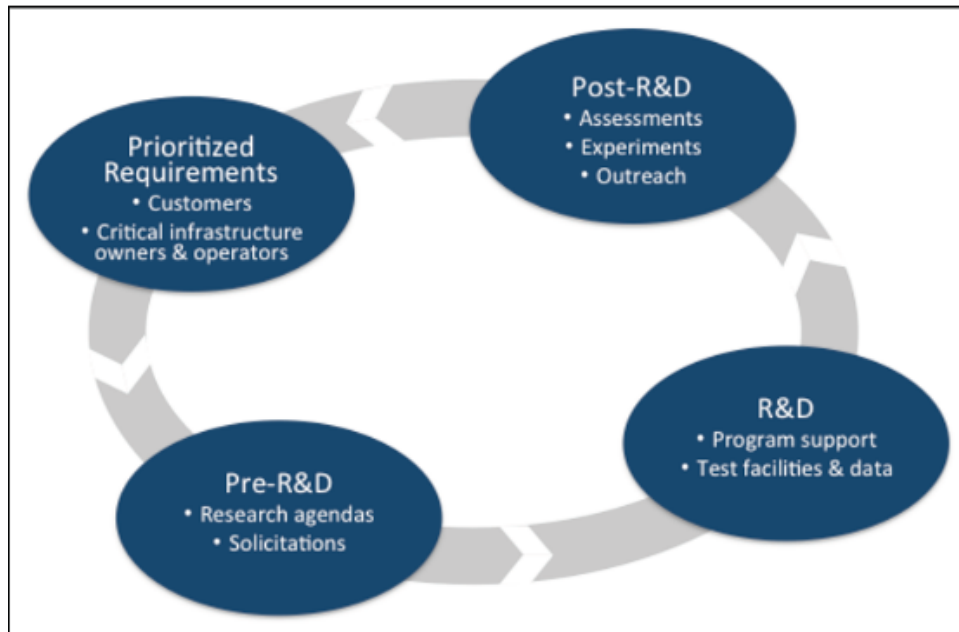


Figure 23: DHS/SRI Cybersecurity R&D Execution Model for Technology Transition

The model consists of the following phases:

1. Prioritised requirements phase:
 - a) Direct interaction between researchers and users which will help the first ones to identify what market can supply and what are the problems which need solution.
2. Pre R&D phase:
 - a) Existence of a research agenda which will help researchers to know what are the problems which the research community is trying to solve and which at the same time will contribute to a team work to be achieved in a global level
 - b) Existence of a solicitation which will consider the technology transition as one of its internal component. In this way transition paths will be implemented very quickly depending on the maturity of the idea which researchers are working on. The levels of maturity can be the nine Technology Readiness Levels (TRLs) for large systems integrations or the three levels (relatively mature technologies, prototype technologies, new technologies) for academics and small start-ups which are a simplified form of the first ones.



Figure 24: SRI's 5 Disciplines of Innovation. All must be present for success.

3. R&D execution phase:

- a) Make sure that the commitment to technology transition is still on
- b) Supply of support and resources to increase the chance of transition
- c) R&D stakeholders participation to ensure that the customer need is driving the program
- d) Providing all researchers and program managers with innovation training such as the Five Disciplines of Innovation framework (Important Customer Needs, Value Creation, Innovation Champions, Innovation Teams and Organisational Alignment)
- e) Ensure that test and evaluation processes are held from the beginning and continue for the duration of the project. This illustrates the need for realistic test data to be examined and necessary infrastructure to be provided, Those can be accessed by datasets such as DETER and facilities like PREDICT

4. Post R&D phase:

- a) Researchers must broaden the scope of their transition activities and expose their technology and tools to a wider audience by technology assessments and evaluations, experiments and pilots, and outreach to potential investors and users. To reach the potential investors, vendors and users; researchers can participate in collective efforts such as community events and technology showcases like the ITTC, SINET and DHS S&T System Integration Forum.

The R&D Execution Model has been applied in the DHS S&T cybersecurity R&D program with successfully transitioned technologies such as the IronKey-Secure USB Memory Device, the Endeavor Systems-Malware Analysis Tools , the Open Information Security Foundation (OISF)-Suricata Intrusion Detection (IDS) Project and many others.

Appendix C EIT institute and its “EIT ICT labs” Knowledge Innovation Community (KIC):

The EIT ICT Labs KIC was established in 2009, and currently comprises many nodes in Europe. Each node is composed of 3 core partner organisations, and a number of affiliate partners. The partner organisations represent top universities leading in ICT, research centres, and global companies. Each node has its unique profile within EIT ICT Labs and encompasses all aspects of the knowledge triangle (ERB: Education, Research and Business). EIT ICT Labs drives the European leadership in ICT innovation for economic growth and quality of life. The main focus of EIT ICT Labs is to reinforce and foster knowledge transfer. Europe has strong positions in research and education in ICT, but the last step, when the research results in ICT are transferred to the market, is not as successful as in other countries, such as the US, therefore knowledge transfer has become one of the main goals of EIT ICT.

To achieve these ambitious goals EIT ICT Labs links the ICT knowledge triangle in Europe, supports the emerging EU-wide entrepreneurial ecosystem, and focuses on the societal challenges in ICT through the selection of innovation areas. In these areas, EIT ICT Labs helps to create new companies, facilitates growth of SMEs, and supports large companies to acquire new innovation capabilities.

There are currently 10 Innovation Areas, also known as Action Lines, promoted by EIT ICT Labs:

- | | |
|---------------------------|---|
| ▪ Future Cloud | ▪ Future Networking Solutions |
| ▪ Cyber-Physical Systems | ▪ Master School |
| ▪ Doctoral School | ▪ Privacy Security & Trust in Information Society |
| ▪ Health & Wellbeing | ▪ Smart Energy Systems |
| ▪ Urban Life and Mobility | ▪ Smart Spaces |

The EIT ICT Labs' investment model is also called a “catalyst-carrier model” and is represented below in Figure 25. It is used to complete the innovation cycle and to reinforce its last step of technology transfer. There are three catalyst types defined and supported by EIT: education catalysts (programs of entrepreneurship education for students to facilitate their integration in the innovation cycles); research catalysts (activities to support research by engaging end-users in it, such as living labs and experience labs); and business catalysts (activities to support companies in acquiring innovation and reaching the market). Catalysts are launched through competitive selections, based on their potential to add value to the EIT ICT Labs goals (and, hence, towards the EU competitiveness).

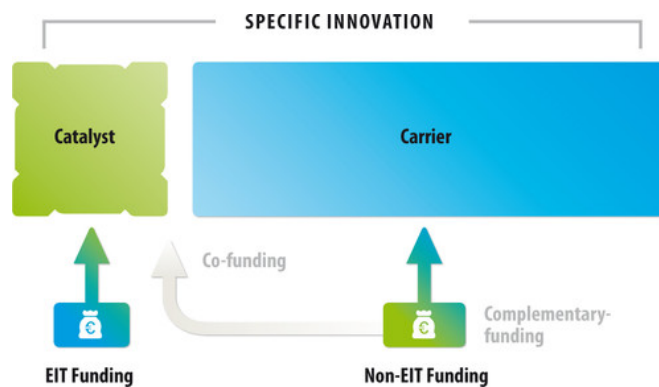


Figure 25 Investment Model of EIT ICT Labs

This approach shows that more innovations can be created with less funding, by leveraging the already existing research results and available technologies. The aforementioned catalyst-carrier model was actually designed with this approach in mind.

To understand the progress of innovation incubation and activities aiming to support innovations, it is necessary to devise **metrics and KPIs** (Key Performance Indicators) that will allow efficient tracking of the progress. EIT ICT Labs use a variety of KPIs, including

- the number of innovations scouted,
- the number of start-ups launched,
- the number of knowledge transfers, and
- the number of innovations incubated.

Research and Education catalysts use similar metrics, e.g.,

- the number of students trained, and
- the number and size of created testbeds.

The identification from the start of the success criteria and the checking of progress at milestones leads to a more sustainable and successful innovation incubation activity.

The following results⁷¹ that EIT ICT LABS achieved in the 2012 are a concrete example of these criteria:

⁷¹

<https://workspaces.ictlabs.eu/site/private/go/article.aspx?id=51&title=Call+for+new+activities+2014>

- 16 New products/services
- 51 Innovation incubations
- 12 New companies created
- 26 Knowledge adoption cases
- 23 Knowledge transfers
- 94 Students in master school
- 40 Students in Doctoral School
- 59 Applications for Doctoral School
- 560 Applications for Master School

These achievements in Education and Research driven innovations come from the activities carried out within the Action Lines ranging from technology maturation to large living lab pilots and standardisation contributions.

EIT ICT Labs has learnt that achieving the ERB triangle is very difficult, particularly the integration phase. In fact, difficulties were found integrating Education with Research and Business because of the original focus on the ERB pillars. As a result, in 2012 EIT ICT Labs decided to improve ERB integration in its Action Lines, with business developers, researchers and students all working together in all Action Line activities. Given the importance of this fundamental integration, additional steps are being taken in 2014 to achieve a deeper integration via Master School Summer Schools in all Action Lines. The involvement of Master and doctoral students in Action Line activities and several measures strengthens the business development.

EIT ICT labs Business and Entrepreneurship has realised that there are different players (individual entrepreneurs, start-ups, SMEs, and large companies) within many communalities and interdependencies and they all have different requirements, so they demand an integrated business development acceleration approach to extract maximum value.

In this direction EIT ICT labs, will in 2014, further develop its Business Development Accelerator that functions as a real pan-European accelerator focusing on pan-European business development beyond the scope of local partners in the EIT ICT Labs ecosystem.

Last but not least, EIT introduced in the Call for Activities 2014 which is the mandatory requirement to justify all activity proposals with an explicit business underpinning with market definition. This process, supported by the allocated EIT business developers, emphasises once again the importance of reducing the time-to-market of the research results.

Taking into account the results it is evident that this model can be very successful at large, and the approach to fund only the last steps to innovation can be used by policy makers.

Appendix D Success stories in European NIS innovation

D.1 NIS innovation success stories at BT

D.1.1 BT Assure Analytics

The roots of this innovative visual analytics technology lie in a £3M BT-led UK Technology Strategy Board project named SATURN (Self-organising Adaptive Technology underlying Resilient Networks) that ran from 2009 to 2012. Other partners were Northrop Grumman Plc, Imperial College and Oxford University. During the project BT developed prototype software based on novel Artificial Intelligence guided search and adaptive visualisation techniques. Its features include multiple data inputs and data type processing, plus the ability to use advanced semantic data matching techniques. The primary application area is the analysis and visualisation of cyber-attacks on enterprise networks and ICT systems, however it has also been applied to a wide range of problem domains including intelligence gathering from social media, network fault diagnosis and retail sales data analysis.

BT Global Services launched a service based on the SATURN software in June 2012, branded as BT Assure Analytics⁷². Assure Analytics is in service in BT's main Security Operations Centre and has also been incorporated into the portal of the BT Assure Threat Monitoring service⁷³. It is a key component of BT's next generation cyber-defence platform for internal and customer use. A wide variety of non-security internal deployments and customer trials are also underway.

Awards and honours include:

- Gold Winner in Innovation in Enterprise Security category at the 2014 Info Security Products Guide Global Excellence Awards
- Finalist in the Innovation category at the 2013 and 2014 SC Magazine Awards, Europe
- Finalist in the Security Innovation of the Year category at the 2013 British Computer Society UK IT Industry Awards
- Finalist in the V3 technology awards in Best enterprise security product and Security innovation of the year categories
- Shortlisted for the Security Excellence Awards in the Cybersecurity Solution of the Year category⁷⁴

Research and development is continuing to enhance the capabilities of BT Assure Analytics via internal projects and the MARS UK TSB collaboration with Bristol University.

⁷²

http://www.globalservices.bt.com/static/assets/pdf/awards/bt_assure_analytics.pdf

⁷³ http://www.globalservices.bt.com/uk/en/products/assure_threat_monitoring

⁷⁴ <http://www.securityexcellenceawards.co.uk/tickets.php>

D.1.2 Security capabilities for BT Cloud Compute platform

The ability to protect IT assets deployed on cloud environments against cyber-threats is a prerequisite to cloud adoption by businesses across the globe and a fundamental element of Europe's cyber-security and cloud strategies.

BT Cloud Compute is a pre-provisioned data centre infrastructure that enables a customer organisation to create, deploy, monitor and manage its own cloud service. A self-service portal provides the customer with the means to set up virtual infrastructure and tailor it to its requirements with near instant provisioning times. Automated delivery allows new services to be launched quickly and efficiently, with high levels of choice, flexibility and control. Cloud Compute can be integrated and managed across hybrid environments. It is being rolled out regionally around the globe.

In order to provide the security demanded by its business customers, BT is developing a number services that will be built into the Cloud Compute platform itself or made available for self-service selection in the same way as application services. The first of these, BT Intelligent Protection: Service Store Edition brings together system security, host and application protection functionality with cloud service management automation in order to protect IT assets, data and applications across multiple cloud platforms. It also hides the complexity of security control integration and security enforcement policy detail from the users, enabling the delivery of security functionality from the cloud into the cloud with a few clicks and without necessitating cybersecurity expertise or specialised knowledge about the cloud or application. It embodies a number of original inventions protected by granted or pending patents.

The solution has been adopted by BT Cloud Compute for product deployment in 16 platforms in 4 continents, 45 data centres, 4 global customer service centre hubs and 22 satellite centres operating 24/7 and serving businesses in 198 countries.

The technology underpinning BT Intelligent Protection was developed by BT Research and Innovation staff in internal and collaborative projects including the FP7 project, OPTIMIS. Collaborative applied research and innovation in the area of cloud security continues in the context of the STRATEGIC FP7 project (addressing local, regional and national government requirements) and the EIT ICT Labs Trusted Cloud High Impact Initiative.

Awards and honours include:

- Finalist in the Cloud Provider Innovation of the Year category (2013 and 2014) and Security Innovation of the Year (2014) at the British Computer Society UK IT Industry Awards

D.2 Security innovation awards and recognition

D.2.1 EY Startup Challenge

In November 2014, consultancy EY launched a new competition in which seven technology start-ups were invited to develop new technologies to solve regulatory challenges like the Right To Be Forgotten (RTBF). The shortlisted companies were as follows:

- Exonar (www.exonar.com) – Exonar allows organisations to understand what information is important, where it is, and who has access to it
- Mentat Innovations (www.ment.at) – Mentat is building a real-time machine learning infrastructure SaaS product
- MyGravity – www.mygravity.co – MyGravity provides consumers a view of their digital self and provides companies a platform of services, products and technology to better use consumers' data
- Privately – www.privately.eu – Privately provides a platform that gives privacy to end-users by allowing them to delete social media posts from circulation
- Sedicii – www.sedicii.com – Sedicii allows identity confirmation without having to reveal personal identifiable information
- Yambina – www.yambina.com – Yambina's Enterprise Data Management provides tools for mapping data sources, applying data transformations and applying rules to data and managing exceptions
- QoiD – www.qoid.com – QoiD provides a secure method for customers to manage and control access to their information stored with someone they trust or self-host

D.2.2 British Computer Society UK IT Industry Awards,

Security Innovation of the Year 2014:

- **Winner:** Gala Tent⁷⁵ – This marquee and gazebo maker won the award for its Secure Order Transfer (SOT) system, developed to help prevent the 48.4m fraudulent e-commerce transactions which take place in the UK each year.
- **Highly Commended:** RandomStorm⁷⁶ -- a UK-based network security, vulnerability management and compliance company, focused on providing enterprise-level, proactive security management products and services to commercial and public sector organisations. It has also been ranked 130th in the Deloitte LLP Technology Fast 500 EMEA and 21st in the Deloitte UK Fast 50, was a finalist in the 2013 SC awards, and a Silver winner of the 2013 Global Excellence Awards in the Vulnerability Assessment, Remediation and Management category.
- **Other finalists:** BT, CipherCloud, GFI Software, FireHost, Clearswift, BT Lancashire Services, Cognia, AirWatch by VMware

D.2.3 SC Magazine Awards Europe⁷⁷

Innovation Award 2014:

- **Winner:** vSentry from Bromium⁷⁸
- **Highly Commended:** Clearswift Adaptive Redaction for Critical Information Protection from Clearswift⁷⁹,

⁷⁵ www.galatent.co.uk

⁷⁶ www.randomstorm.com

⁷⁷ <http://www.scawardseurope.com/results-2014>

⁷⁸ www.bromium.com

⁷⁹ www.clearswift.com

- **Finalists:** Assure Analytics from BT, Check Point ThreatCloud Emulation from Check Point, Innovation from Darktrace, SIEM and Security Intelligence Platform from LogRhythm, WebLife Balance from WebLife Balance LLC

D.2.4 Computing Security Awards⁸⁰

New Product of the Year category 2014:

- Winner: Wallix - WAB On Demand
- Runner-up: Skyhigh Networks - Skyhigh Cloud Security Manager

D.2.5 Deloitte Technology awards

NIS companies in 2014 UK Fast 50:

- Avecto⁸¹ (4, North West Regional Winner) – a provider of Windows Privilege Management technology.
- HighQ⁸² (50) - HighQ Collaborate combines secure document management with enterprise social collaboration tools.

NIS companies in 2014 EMEA Fast 500:

An annual ranking of the fastest growing technology companies in Europe, Middle East and Africa (EMEA).

Unfortunately the published list⁸³ does not provide descriptions of the companies, and the industry sector is not broken down sufficiently to allow NIS vendors to be identified. Avecto, mentioned above in the UK Fast 50 list appears in the EMEA list at 32, and HighQ appears at 312. Other companies recognisable as NIS vendors include:

- Checkmarx⁸⁴ (Israel, 127) Static analysis of source code
- Waterfall Security Solutions⁸⁵ (Israel, 335) Cybersecurity for industrial networks and critical infrastructures.
- SecureLink⁸⁶ (Netherlands, 416)

D.2.6 Gartner Cool Vendors in Security for TSP⁸⁷

The following Cool Vendors in Security for Technology and Service Providers were listed for 2014:

⁸⁰ <http://www.computingsecurityawards.co.uk/>

⁸¹ <http://www.avecto.com/>

⁸² <http://highq.com/>

⁸³ <http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-emea-f500-2014-ranking.pdf>

⁸⁴ <https://www.checkmarx.com/>

⁸⁵ www.waterfall-security.com

⁸⁶ <http://www.securelink.nl/>

⁸⁷ Cool Vendors in Security for Technology and Service Providers, 2014, 11/4/2014, Gartners

- Agari⁸⁸ (US), a relatively new start-up company that focuses on leveraging big data analytics on 4.5 billion emails per day derived from the use of the DMARC security framework for email senders and receivers.
- Dome9⁸⁹ (Israel) has built partnerships with hosting providers and is effectively using them as a route to market for its products.
- Netmonastery⁹⁰ (India) provides a real-time threat management platform to hosters and telecom providers to enable them to build out managed security services and/or threat intelligence capabilities.
- SecurityMatters⁹¹ (Netherlands) has developed innovative network monitoring technology, which provides situational awareness and continuous control, helping to identify misconfigured and rogue devices and (unwanted) changes in current configurations, and detecting human errors and threats, such as new and unknown (zero-day) cyberthreats and even targeted attacks. These security controls bring a better understanding of traffic patterns within the complex critical infrastructure networks in order to detect malicious attacks and other anomalies.

The note also contains a follow-up account of a company profiled in "Cool Vendors in Data and Infrastructure Protection, 2010". Boole Server⁹² (Italy) was selected as a Cool Vendor in 2010 because of its easy-to-use data protection capabilities and the breadth of functionalities reaching across disaster recovery management, data loss prevention, device control and disk-file encryption. Over the past three years, at the product level, Boole Server has expanded delivery capabilities through a Web-based interface, expanding also to key mobile platforms, such as iOS and Android. Boole Server has strengthened its geographical presence and currently generates 50% of its business from international clients, including international police forces, law firms and financial institutions.

D.3 IPACSO innovation awards - Research and Innovation in Sedicii

In October 2014 the EU-supported research project named Innovation Framework for Privacy and Cyber Security Market Opportunities (IPACSO), hosted EU's First Cyber Security & Privacy Innovation Awards.

Europe's most innovative and forward-thinking researchers and entrepreneurs gathered in Brussels on 23 October 2014, recognising those who are bolstering Europe's cyber security landscape. The following company Sedicii was one of the award winners.

Company Overview: Sedicii Innovation Limited is an early stage start-up founded in 2013 which spun out from academic research and government sponsored commercialisation supports. Sedicii pioneers "game changing" technology

⁸⁸ www.agari.com

⁸⁹ www.dome9.com

⁹⁰ www.netmonastery.com

⁹¹ www.secmatters.com

⁹² www.booleserver.com

eliminating the need to transmit or store private information (e.g. passwords, credit card details or a passport number) for authentication purposes. Based on the Zero Knowledge Proof protocol and innovative graph theory, applications include single sign on authentication for applications or embedded devices, credit card tokenization, and identity attribute verification.

Sedicii Innovation Path: The basis of the Sedicii Technology was conceptualised during a 5 year Research & Development programme in DERI in the National University of Ireland Galway. There were two primary motivations for the research performed in developing Sedicii. Firstly, the growing demand for secure technologies for e-commerce that do not put customers at risk of identity theft and secondly, the escalation of Web 2.0 and the social semantic web leading to new business models in terms of way that user's interact with the web.

Recognising the commercial application and market potential of the innovative Sedicii Technology, an experienced technology entrepreneur (now CEO of Sedicii) spearheaded the commercialisation of the innovative research outputs. Commercialisation activities began in Spring 2013 with securing a commercialisation grant from Enterprise Ireland (the Irish enterprise development agency). This facilitated the first stage of commercial activities to begin transforming the technology into a product. The technology was subsequently spun out into a new company called Sedicii Innovations Limited. The team includes a CEO, Global Commercial Director, UK Country Director and CTO, all of which bring extensive technology and business development acumen to accelerate the on-going growth of the company. Protected with a US patent and EU patent application, the Sedicii technology is currently being evaluated by BT and Gemalto in France and a diverse range of use cases across a number of sectoral verticals are being validated.

Sedicii's entrepreneurial and business development team's current innovation foci is on raising seed finance, refining the value proposition and establishing the Sedicii message and bringing the technology to market in the form of various products. In the last year Sedicii has secured commercialisation funding at an Irish national level and most recently via the H2020 SME instrument. In addition to this, the team has secured international brand recognition and development supports through participating in, being finalists and winning numerous prestigious awards including but not limited to: EY Startup Challenge, BT Infinity Lab London UK, Matchi Global Fintech Innovation Challenge, World Cup of Tech in Silicon Valley, Techcrunch Disrupt New York City, Innovative Privacy Company at EU IPACSO Awards, Next Bank Europe Innovation Awards, Paypal Sponsored Startup of the Year, Cisco IoT Grand Challenge and R&D Collaboration of the Year at the Irish IP Awards.

Sedicii's authentication technology is positioned for high volume market opportunities, supporting the needs of all digital authentication and payment processing underpinned by enterprise licensing and cloud based "authentication as a service" business models. Sedicii is currently pursuing a strategy of partnering with organisations of significant market sizes in a particular vertical and to use the distribution channels of those companies to push the product to market. The company was successful in securing a place on the Oxygen Accelerator in London as one of eight companies selected from an application pool of over three hundred.

Representing a cross-disciplinary innovation path involving academic researchers, entrepreneurs and business development professionals, and national and international funding and enterprise agencies the Sedicii story represents a superb example of how government supported academic research can be successfully commercialised through the provision of carefully targeted funding and supports.

Appendix E High impact use cases: examples from applying the methodology

This section contains a collection of descriptions of scenarios with challenging security requirements proposed by contributors to this study, such that meeting those requirements will have significant societal or economic benefit. It is important to remember that these are use case scenarios and not descriptions of research topics. The idea is that we will end up with a list of research goals that can be justified (at least in part) because they are derived from (and can be traced back to) high-priority security requirements that are currently not met. Thus the logic of this part of the report leads from stakeholder concerns, to use cases that make those concerns concrete in specific scenarios, to capabilities/services that would address those concerns, from which we can define research goals by generalisation or identifying enabling advances. Note that ideally there would be a many-many relationship between scenarios and research goals, and research goals that affect multiple scenarios will be ranked higher in terms of impact.

The following was the guideline given for the contents and structure of a use case description, though not all contributions follow it rigidly:

1. Description of setting
2. Dramatis personae (description of stakeholders and threat agents, etc.)
3. Main security concerns of stakeholders that are currently addressed inadequately
4. New (hypothetical/abstract) services that would solve the problem
5. Required enabling technologies / capabilities
6. Assumptions / dependencies

The use cases are not intended as a complete set of security scenarios, rather, they are a collection of representative examples from which we can generalise.

E.1 Security for Internet-of-Things Infrastructures

E.1.1 Description of setting

Currently, the Internet of Things (IoT) is emerging as a major driver of the IT Landscape. Billions of connected devices structured in systems of systems as well as intelligence (sensing, analytics, and actuation) will drive major opportunities for the European IT Industry.

Unlike traditional IT systems, IoT drives new requirements into the market. Examples include:

- Billions of devices owned and managed by millions of authorities
- Lightweight hardware operating under strict power constraints limit the capabilities of the end nodes.
- Intelligence and infrastructures are likely to break down today's silos per Industry/Sector. Instead, analytics and control will be possible across disconnected industries such as logistics and manufacturing.
- Long-term deployments where sensors and devices are deployed in the field today and are likely to operate for 20+ years.

While IoT systems are rolled out today, security is largely ignored. Due to cost, power, or other constraints, many deployments have either minimal security or none at all.

E.1.2 Dramatis personae

The IoT landscape includes many stakeholders. In general, the whole economy can be affected by failure of IoT Systems. For each sector, a detailed list of stakeholders can be identified. At a high level, they can be grouped in the following categories:

- **Citizens:** The citizens that receive services and whose privacy may be affected by failures and privacy incidents.
- **Governments:** IoT systems will control large portions of the infrastructure of a country. As a consequence, governments can be affected by failures of those systems.
- **Industry:** Similarly, companies will increasingly rely on IoT systems and their failure will lead to substantial economic damage.

E.1.3 Main security concerns of stakeholders

Today, IoT systems that are deployed in the field often lack the most basic security capabilities. Severe risks for all stakeholders result from this absence of security.

Citizens raise multiple concerns:

- **Privacy invasions:** Unauthorized eavesdropping or data collection by the large numbers of Internet-enabled devices
- **Service disruptions:** Due to lack of security, the availability of services may be at risk. In particular for critical infrastructures such as logistics or utilities, the insecurity of the underlying components constitutes a substantial risk.

Governments face similar concerns:

- **Reduced resilience** of an economy due to IoT systems as single points of failures.
- **Espionage** and mass surveillance based on the data collected by IoT systems.

For enterprises, concerns include

- **Safety:** Once physical devices are controlled by Internet-accessible systems, safety is a substantial concern.
- **Secure life cycle management:** How to protect IoT devices along their whole life-cycle. This should include legacy devices as well as devices with a long life time.

While IoT provides gains in efficiency and allows instrumentation of a wide range of systems, the available technologies still pose substantial security risks.

E.1.4 New services that would solve the problem

In order to address these risks, progress needs to be made along multiple dimensions:

- **End-to-end Security:** Practical concepts that provide end-to-end protection of IoT systems. This would, e.g., enable the protection of confidentiality and the integrity of data from the sensor into the cloud.
- **Scalable Protocols:** Most of today's security protocols do not scale to large numbers of devices (at reasonable costs). Whenever a device is added, corresponding cloud resources must be added, too. A challenge is to develop protocols that can scale with zero cost increase per devices.
- **Lightweight Security:** In particular for tiny sensors, all security mechanisms need to be lightweight to be implemented in a cost efficient way. This can include lightweight HW as well as algorithms optimized for low cost systems.
- **Migration path for legacy systems:** For the wide range of legacy systems, an important challenge will be to design a migration path from the status quo into a secure system of systems.

E.2 Advanced infrastructures for supporting secure and privacy-preserving data management and governance at scale

E.2.1 Description of setting

Increasing available data volumes facilitate increased analytical and value-add possibilities from information. However, this rapid increase in data volumes is making it increasingly difficult for organisations to govern their data effectively. Organisations are finding it more difficult to gain appropriate governance and oversight over their data and content, understand what data they have, what data is being retained, if valuable business data is being ignored and whether data is managed in a compliant, secure manner. Without proper consideration, there are potentially serious consequences to the organisation if left unaddressed. Benefits of any effort also need to be aligned with business objectives to ensure it is clear what value this will deliver to the business.

In the context of a typical large organisation, this data proliferation involves multiple business units and stakeholder perspectives, often in a highly distributed context involving multiple regions, with data/content potentially involving multiple languages. Such an organisation may experience a sudden trigger event which requires a fast and efficient data consolidation exercise, for example in response to a legal requirement, an audit event, a compliance mandate, or in order to solve a HR issue or other operational challenge. However as many organisations are unprepared, performing such a task at short notice can be problematic. A rushed data gathering exercise is pursued in a panic, leaving relevant custodians of such data disgruntled and on guard about such intrusions. Crucial data may be omitted from the process due to procedural or technological shortcomings. Technical/IT personnel may grapple with understanding domain-specific concepts in order to complete the task. Security and privacy policies are violated, and conformance with compliance mandates and regulations are often compromised during the data gathering effort. In particular, significant amounts of time, effort and interruption are expended, leading to significant discovery costs.

Hence there is a need to develop improved means of supporting distributed data sharing, collaboration and governance at ever-increasing scale. A key perspective

within this is to ensure that data security, privacy and adequate organisational Information Governance (IG) is maintained, especially as increased amounts of organisational data are being shared with and managed by third-parties in line with increased use of cloud computing.

E.2.2 Dramatis personae

Organisational Information Governance is ultimately a process driven endeavour involving multiple stakeholder perspectives including IT (e.g. Chief Information Officers, data architects, Extract, Transform, Load (ETL) staff), security and risk management, and operational business users of datasets among others. IT users and business users with domain expertise will typically work in concert to ensure that data is managed effectively. Key IG stages at a broad level include:

1. Identifying sources and locations of organisational data across IT infrastructure
2. Classification and prioritisation of that data, and definition of priority projects
3. Managing and optimising the data to reduce risk and increase business value, setting of appropriate data management and usage policies
4. Monitoring and improving the overall IG process.

External third-party expertise around security, risk assessment and data management aspects of the IG process may also be leveraged. Relevant threat agents may exist both within and outside organisational boundaries, chiefly due to gaining unauthorised access to information. A broad range of national, pan-national and industry specific regulations, as well as internal compliance policies, provide guidelines to ensure that efforts are put in place to enforce necessary security and privacy controls.

E.2.3 Main security concerns of stakeholders

Several broad challenges to secure collaborative data management in a distributed infrastructure context exist, e.g.:

1. Ensuring that security is not compromised when different organisations and data sources in different jurisdictions/locations have different rules around aspects such as data protection and retention policies, classification levels, unique compliance mandates and access control regimes.
2. Implementing the correct privacy safeguards to ensure that only allowed data is transferred between organisations, and data is protected at different levels of granularity
3. Difficulties in ensuring a consistent updated data version is being used across distributed collaborators and that updated data versions are not lost
4. Communication issues relating to bandwidth, connectivity and latency when transferring data
5. Correct classification and prioritisation of critical data assets, and the ability to identify when data violations are occurring
6. Allowing different institutions with different technologies, data workflows and different underlying data models to collaborate effectively

Achieving a correct balance between centralising and combining distributed datasets to support efficient data analysis, while in turn preserving data protection and security principles is a difficult balancing act. For example in existing manual

scenarios, distributed datasets that are aggregated and centralised may lead to sensitive data units whose location coordinates are no longer known, leading to potential violation of data privacy principles as they presently exist, and increased security risk. At the other extreme, strict organisational policy may only allow data to ever be accessed at its physical location, meaning that data units cannot be relocated when it may otherwise be favourable, increased complexity in de-duplicating unnecessary data, and having costly consultants being moved around to physical locations leading to increased overhead and inefficiencies, when remote management and access to relevant data may have been more favourable.

E.2.4 New services that would solve the problem

What is ultimately needed is improved technology infrastructure for supporting secure and privacy-preserving data management and governance at scale and in a distributed infrastructure context.

Potential service features within such an infrastructure could include:

- Clustered review platform with ability to deploy multiple processing and review nodes across multiple locations needed to fit the distributed data management scenario.
- Ability to preserve connections between central master node, and nodes in different jurisdictions, allowing system settings, user accounts and other global case data to be kept consistent, allowing all of the team members to be working off of the same data management case, even if they are not allowed to view some of the documents
- Ability to selectively prevent relevant data (metadata or otherwise) from being viewed between central and remote case nodes, and to release data between nodes once various data management (e.g. processing/review) stages are complete
- Support the setting up of asynchronous permissions for example the team in one jurisdiction (X) may not be able to see the data in another remote jurisdiction (Y), but the team at Y is allowed to see the data at X. Even if total segregation is enforced (neither team can see each other's data) deduplication can still be achieved by allowing the Hash signatures of the documents to be sent across the shared link, preventing reviewers from looking at documents twice. This would allow investigators to have a single case, regardless of where the data is, but also give assurances that the data is not transferred across boundaries/jurisdictions without authorisation.
- Searchable encryption features so that data can be pushed to remote locations (e.g. public cloud infrastructures if needed), limiting access to that data at the physical location while facilitating remote data analysis and processing.
- Appropriate data classification mechanisms to support identification and prioritisation of critical high-priority data, and DLP-like functionality to identify when violating data extrusion (or similar) events are occurring.

E.2.5 Required enabling technologies / capabilities

- Leveraging of emerging cloud management platforms to support instantiation, deployment and dynamic reconfiguration of necessary distributed data management infrastructures

- Better integration between cloud management platform and available data management and analysis technologies, such that necessary data management technology instances can be deployed and reconfigured as needed, supported by adequate workflow engine support
- Support for data security around distributed datasets (e.g. searchable encryption techniques)
- Improved infrastructure orchestration tools beyond focus on deployment of structural infrastructure aspects, but also to include support for dynamic security and privacy policy generation as part of overall distributed data management infrastructure deployment

E.2.6 Assumptions/Dependencies

A number of risk factors may need to be managed in order to support uptake of more advanced distributed data collaboration. These might include:

- Trust issues among target data management stakeholders around allowing increased use of technology to manage privacy/security of data, and a preference to rely on traditional approaches even if they are economically unsustainable.
- Regulatory issues (national or industry-specific) that may prevent or hinder organisations from adopting for advanced data sharing practices, and the shifting legal landscape around data protection issues at a national and pan-European level.
- Cultural issues around acceptable norms around data practices and sharing, varying potentially by organisation, nuances of target market domain (e.g. varying IG and eDiscovery practices) or national psyche.

E.3 Data Business: Data becoming the major business asset and the foundation of new businesses

E.3.1 Description of setting

Three major recent trends have led to improving existing businesses and opening up new business opportunities based on the analysis of large amounts of data, leading to previously unknown scale and precision of results (correlations, forecasts, visualisations, etc.):

- Creation of data. Data production is still growing exponentially, particularly powered by the “prosumer” approach and the inclusion of data about the physical environment through the Internet of Things and machine-to-machine communication.
- Availability of data. Many of these data are publicly available and can be easily consumed (e.g., Open Data)
- Processing capabilities. Hardware and software improvements, including processor power, in-memory computing, columnar data bases, massive parallelism etc. allow these data to be processed in real-time.

The increased value of data for business is exemplified by services that are offered for free to their users (e.g., search engines and social networks) and which build their business models on the collection and usage of data about users and their behaviour (e.g., targeted advertising). Other examples include the improvement of

commercial offers based on the analysis of feedback through public channels and the provision of value-added services based on location data.

However, many of these data including personal data are of a sensitive nature, or become sensitive / change their sensitivity when being aggregated (e.g., profiling, location tracking). Hence, there is a need for assessing the sensitivity of collected and traded data in the context of their particular usage and the different stakeholders' requirements on their security and privacy. Simply restricting the access to data or controlling the purpose for which they are processed limits the business opportunities, since the most promising of them are based on creative new usage and combination of the collected data. In fact, Big Data aims at analysing large amounts of raw data to identify previously unknown correlations, patterns and usages.

E.3.2 Dramatis personae

Since the protection needs in this scenario are related to the data that is created, collected, published and processed, the main stakeholder roles stem from their relation to the data. Hence, typical roles can be taken from the ones defined in the data protection regulations: data owner, data controller, data processor.

E.3.3 New services that would solve the problem, and required enabling technologies

The major difference between the data business scenarios included here and the traditional ones lies in volume of the data, the diversity of its sources, the inclusion of unstructured data, the storage on shared infrastructures including the cloud, the complexity of service supply chains, the dynamic context, and the unpredictable nature of their intended usage. Existing technologies including privacy policy languages, PETs, usage control, anonymisation/pseudonymisation of data, randomisation, inference control etc. address the stakeholders' protection needs, but are subject to restrictions on the context or the type of processing of the data. For instance, anonymisation techniques like k-anonymity or l-diversity assume that the anonymised data set is closed and its statistical properties known. However, the continuous creation and improved accessibility of data might violate these assumptions, since a data processor might have access to external sources and data which properties allow for additional inferences. As another example, big data application might benefit most from raw data since they allow for the identification of previously unknown interesting relations.

New services and technologies, hence, need to address extended usage contexts and go beyond the restrictions / assumption of the existing ones. Such services may include:

- Risk assessment and management services targeted to data controllers and processors that support the evaluation of their business models and data collections as well as ongoing data operations
- Transparency services that allow data owners to get aware about the state of their data
- New anonymisation schemes for data sets that relax/reduce assumptions on anticipated operations performed on them
- Encryption schemes with algebraic properties beyond homomorphic encryption

- Data quality and provenance services
- Practically feasible approaches (including frameworks and platforms) to include such services in software applications and systems
- Services to automate / support privacy impact assessments, including the deployment of technologies mitigating identified risks

E.3.4 Assumptions/Dependencies

A number of risk factors may need to be managed in order to support uptake of more advanced data business. These might include:

- Trust issues among target data management stakeholders around allowing increased use of technology to manage privacy/security of data, and a preference to rely on traditional approaches even if they are economically unsustainable.
- Regulatory issues (national or industry-specific) that may prevent or hinder organisations from adopting for advanced data businesses, and the shifting legal landscape around data protection issues at a national and pan-European level.
- Cultural issues around acceptable norms around data practices and sharing, varying potentially by organisation, nuances of target market domain or national psyche.

E.4 Stealthy industrial espionage by APT

E.4.1 Description of setting

The scenario is set in the Security Operations Centre of a multi-national enterprise. One of the threats facing the enterprise is theft of valuable intellectual property by agencies sponsored (with plausible deniability) by foreign states aiming to give their own industry a competitive advantage. The threat agents are well trained and well-funded and shielded to a degree from prosecution, retaliation and other sanctions by their state sponsors. They are prepared to be patient and play a 'long-game' to gain their objective. They take care to avoid detection while penetrating defences and compromising systems, and once an exfiltration route is established will cover their tracks, e.g. by editing log files. They may leave the compromise in place, using it repeatedly over a number of years. Even if the compromise is detected it may be difficult to work out how and by whom it was effected. Although the main motivation considered here is intellectual property theft, the possibility of sabotage also cannot be ignored.

The potential financial impact is enormous. Proprietary technology resulting from large multi-year research programmes represents a huge investment, and if competitors are given access to it, the expense is incurred without yielding a competitive advantage. Even relatively minor leaks, such as of details of a competitive bid for a valuable contract, can have multi-million pound consequences.

With today's state-of-the-art, the advantage is definitely with the attacker. Multiple penetration routes are available to the attacker, who only needs to find one way in to succeed. Many of these routes currently involve manipulation of the behaviour of people with legitimate system access to gain the initial foot-hold. Detection of compromise is difficult, and no organisation can assume it is free from back-doors.

When a compromise is detected, it is usually well after the event, so that the attacker has a sizeable window of opportunity during which to exploit it, and the company may not know what assets have been stolen. Even if the perpetrator is identified, gathering enough evidence for a prosecution is problematic, and in any case, the perpetrator, may be effectively outside the reach of the law.

E.4.2 Dramatis personae

- The enterprise's cyber-defence operations (CDO) team, responsible for anticipating, pre-empting, combatting, recovering from, and investigating attacks.
- The attackers: a shadowy team of talented, well-trained, well-funded, highly motivated individuals sponsored (deniably) by a foreign power and operating from its territory.
- The enterprise's board, which is responsible for allocating budget and defining risk appetite, and is accountable to shareholders.
- Legitimate users of the enterprise's IT systems, who may be manipulated by the attackers.
- CDO teams in other enterprises facing similar challenges
- Cyber-teams in defence, intelligence and law enforcement agencies concerned with protecting civil society and national economy
- Oversight agencies and civil liberties bodies concerned that citizens' rights might be violated in the course of combatting APTs.

E.4.3 New services that would solve the problem

The CDO team needs an integrated suite including the following tools/services:

- Cyber-threat service providing up-to-date information and predictive intelligence on active threat groups, their motivations, targets, techniques used, etc. This service makes use of information feeds from a variety of sources, including peer CDO systems in other enterprises, defence, intelligence and law enforcement agencies, cybersecurity vendors/service providers, monitoring of news and social media, etc. The intelligence is provided in a form suitable for human consumption and also in a form that can be consumed by other tools in the CDO suite.
- A service that can detect and characterise stealthy attacks at various stages with low false positive and false negative rates. Based on the characterisation (in combination with threat intelligence and other contextual information) it will predict likely ways in which the attack will develop and how the attacker will respond to countermeasures. It will trigger appropriate autonomic defensive processes (subject to policies and safeguards limiting the scope of autonomous action), alert human operators, and provide them with means to monitor the progress of the defensive action and intervene if necessary.
- A service looking outside the enterprise to detect indications that proprietary information has leaked and working out likely ways in which it was exfiltrated.
- A forensics service that operates during and after an attack identifying the perpetrators and gathering evidence that enables action to be taken against them.

- A recovery service that repairs the effects of an attack and restores normal operation as soon as possible.
- A learning service that examines attacks retrospectively, draws lessons from them and uses them to update the defensive services, improving their performance and allowing them to adapt to changes in the behaviour of threat groups.
- A service generating indicators allowing the performance of the overall CDO suite and its components to be tracked and appropriate action to optimise risk exposure with respect to other enterprise performance measures.
- A compliance service providing auditable evidence that policies, regulations and guidelines have been followed, and enabling the enterprise to be certified as having a particular security competence rating.

E.4.4 Required enabling technologies / capabilities

Providing the above services requires:

- Large amounts of heterogeneous structured and unstructured data to be collected, correlated and reasoned about using domain and contextual knowledge, to synthesise a coherent picture of the enterprise and its environment from a cyber-defence perspective. This implies large-scale application of artificial intelligence, machine learning, and related techniques in a time-critical setting. In the case of stealthy attacks, the problem is particularly demanding
- Trustworthy autonomous operation. In many cases, a timely response will not allow time to consult a human operator, but there is a strong risk of negative impact if wrong action is taken. The system must be aware of the bounds of its authority (rules of engagement), its own limitations, and of the possible/likely consequences of its actions.
- The ability to reason tactically about the likely behaviour of an able opponent, and out-think and out-respond him.

The pace of change in technology, business practice and threats means that any static CDO suite would rapidly become out-dated and ineffective. On the other hand, it would be extremely expensive to replace the suite on a regular basis, and the enterprise would be exposed or suffer costly downtime during the replacement activity. The owner/operator will want to combine components from different providers on a best-of-breed basis to obtain the best overall match to its security requirements at any given time. We expect continued rapid innovation in defensive technology and weapons and tactics used by threat agents. Consequently, the CDO suite needs to be highly modular and flexible and designed for continuous evolution of capability. It should be based on open standards and reference architecture, but this need to be carefully established to promote rather than discourage innovation.

E.4.5 Assumptions/Dependencies

The above solution focuses on tools and services to anticipate, detect and respond to threat activities. To shift the balance in favour of the defenders, such tools need to be accompanied by improvements in:

- the vulnerability and robustness of enterprise processes, applications, middleware and infrastructure;

- the threat/risk awareness and behaviour of human participants in business processes;
- the compatibility of human and technical elements involved in business processes to avoid.

There are legal, ethical and political/diplomatic issues surrounding offensive operations against a cyber-threat even when clear evidence is available. Consequently, such a capability was not included in the list of services.

E.5 The Insider Threat

E.5.1 Description of setting

The term “insider” is usually used to describe someone holds legitimate access to an organisation's assets and who abuses that access to commit an unauthorised act. Insider incidents may be perpetrated by deliberately or accidentally and may even be unwitting, where an employee may be recruited or duped into committing an unauthorised act on someone else's behalf. Insider acts may be conducted to support criminality (e.g. fraud or theft of sensitive information), terrorism (e.g. leaking details of terrorist targets) or corporate/state espionage (e.g. theft of technical secrets). These incidents can have significant impact on the victim organisation, such as public embarrassment, loss of competitive advantage or even the destruction of property.

Insider activities can take a multitude of forms, however research by the Centre for the Protection of National Infrastructure (CPNI) has identified 5 main types of insider activity: unauthorised disclosure of sensitive information; process corruption; facilitation of third party access to an organisation's assets; physical sabotage; and electronic or IT sabotage. The most frequent types of insider activity tend to be unauthorised disclosure of sensitive information and process corruption, and more often than not, when insider threats occur, this is usually self-initiated. The CPNI report identified the case of a senior finance manager with over 10 years' employment who committed an insider act of process corruption by enabling payments totalling over £250,000 to be made to a personal bank account. The manager manipulated the system to ensure that he was the single point of authorisation for all salary payments made via a third party managing the organisation's payroll. When asked by the Directors to provide a set of accounts showing the salary payments, the manager gave excuses for the unavailability of certified accounts and provided his own spread sheets showing salary payments across the business. These spread sheets were doctored to show the insider's salary recorded correctly, and the additional payments spread across all other employees. The manager, with an over-inflated sense of his own value and contribution to the organisation, increased his own salary and claimed overtime payments without oversight or authorisation from another employee. At the same time he established systems to ensure that all questions relating to the payroll were directed to him to avoid anyone within the organisation uncovering his actions. The manager's actions were only discovered after he resigned from the organisation. The financial damage inflicted on his employer and colleagues was severe and resulted in a need to reduce staff and services in order to avoid bankruptcy. The

manager was able to commit this act because his position gave him the information to know how these systems work and the access to corrupt the process.

E.5.2 Dramatis personae

The stakeholders affected by an insider incident can vary. They may include the Chief Information Officer of the organisation, shareholders, security and risk managers, other members of staff and the end user/customer. Insiders may act alone, or may act on behalf of external parties, such as criminal gangs or foreign governments. The core issue is unauthorised use of legitimate access to an organisation's information and systems.

E.5.3 Main security concerns of stakeholders

The CPNI study on insider activity identified the following key factors that can increase the risk of an insider incident:

- A lack of sufficient management supervision or oversight of employees which can make it difficult to spot indicators of insider risk, such as poor relations with colleagues, absenteeism or anti- social behaviour
- Poor usage of auditing functions within an organisations IT systems thus making it difficult to spot unusual behaviours
- Lack of appropriate protective security controls for controlling how employees introduce or remove organisational data and/or manipulate organisational information remotely. A lack of segregation of duties is often found in evidence in process corruption cases
- A poor security culture is often present in areas where insider activity takes place and there is a lack of adherence to security policies and practices by employers and with management being unaware of these malpractices
- Poor communication between business areas can often result in the inability of the organisation to be able to make an effective risk assessment or enabling it to misjudge the risk that's being carried out
- Inability of the organisation to carry out adequate personnel security can result in employees being placed in roles likely to make them more vulnerable to compromise due to a variety of reasons including a lack of skill, experience or aptitude for the role.

E.5.4 New services that would solve the problem

Some of the measures/controls, which could help mitigate the risk from insider activities, can include:

- Monitoring tools that can intelligently detect malicious insider activities (and insider- related deviations from normal behaviours)
- Development of appropriate risk management tools which can help HR managers identify staff that are more likely to engage in insider activity
- Developing widely available educational material, toolkits and strategies (plug and play materials) which organisations can incorporate into their organisational risk and insider threat prevention models
- Developing a visual analytical interface, which can assist organisations to make complex decisions by enabling a better understanding of which roles within the organisation are most vulnerable to insider threats.

E.6 Effectiveness of security controls mitigating IT risks: From qualitative to quantitative benchmarking

E.6.1 Description of setting

In the cybersecurity field, emphasis on regulatory and technical compliance has far outweighed results regarding effectiveness of controls to thwart cyber-attacks. However to rectify this abnormal situation (unique in the business world, if we think especially of quality, communication, safety and physical security), we need clear and relevant landmarks linked to general reference frameworks (such as ISO 27002, Cobit DS5, CAG Consensus Audit Guidelines) and aligned to business objectives.

So, to practically implement that, one of the most frequently unmet requirements is the **lack of relevant top-down approaches and related operational standards** in IT Security measurements, a key issue at the convergence of 'Measurable security', 'Governance' and 'Standards'. These requirements concern especially:

- All market sectors,
- Owners and operators (of the ICT-based system),
- Security technology provider, system integrators and service providers.

E.6.2 Dramatis personae

- CISOs for an effective IT security governance
- The enterprise's board, which is responsible for allocating budget and defining risk appetite, and is accountable to shareholders.
- The enterprise's cyber-defence operations (CDO) team, responsible for detecting security incidents and weaknesses
- Legitimate users of the enterprise's IT systems, who may be made more aware on their risky behaviours when presented with real hard figures
- CDO teams in other enterprises facing similar challenges
- Cyber-teams in defence, intelligence and law enforcement agencies concerned with protecting civil society and national economy

E.6.3 New services that would solve the problem

An organization's management require a high level of assurance through the **continuous assessment of the organization's security posture**, which will become more and more mandatory in a setting where:

- Increasing use of external or personal IT resources raises new challenges,
- IT security threats are constantly increasing and evolving and people are key (involved in 70 % of all cybercrime-related security incidents),
- Most attacks are the result of organized groups with precise objectives.

In this unstable and more complex environment, the main stake and challenge to overcome for organizations is to keep mastering their information systems.

The best and only way to provide the desired level of assurance is to **position trust tools on the information system**, which will 'stabilize friable matter' and act as 'bars in reinforced concrete'. We can list the 3 most important ones: identity and access management (employees and partners), PKI, operational indicators measuring deviant behaviours and biases against accepted residual risks.

This third means is therefore about using a governance tool making it possible for the management to continuously assess the IS security level. This measurable security aims at helping to respond to the following issues:

- Are the organization's practices compliant with its security policy or ISMS (Information Security Management System) and with what level of enforcement?
- Are existing security measures and tools effective?

These two issues can be dealt with in a harmonized and common way by relying on a **reference framework** (at least security event classification model and related set of operational indicators) based on several key features:

- Even emphasis on security incidents and vulnerabilities/non-conformities,
- Event-centric approach (continuous monitoring and checking),
- Clear correspondence with the organization's risks (IT risk profiles) and Information Security Management System (for example ISO 27002 or NIST 800-53 controls).

Standardization on this matter is essential because such a set of indicators or measurements (typically 80 to 100) has to be proven by sharing of experience and has to be widely published in order to stimulate sharing of statistical state-of-the-art figures within the Cybersecurity profession. Such new standards and reference frameworks could make it far easier for organizations in Europe to:

- Benchmark themselves with state-of-the-art figures (possibly available through large public data bases) and accurately assess their security posture,
- Identify security events and be able tomorrow to notify them accurately to relevant regulatory and enforcement bodies (Cf. breaches and related information),
- Provide cyber insurance companies with the necessary figures to help them work out the right coverage.

Several standardization or user sector and industry or research initiatives or projects are heading to providing new landmarks in this field, such as:

- CYSPA (European Cybersecurity Protection Alliance), initiated by 17 founding organisations to increase the capacity of industry to protect itself from cyber disruptions, and to support the European elaboration of regulations to enhance the overall protection level,
- CAPITAL (which complements the CYSPA project), a collaboration between 9 research organizations led by EOS and aimed at coordinating European R&D efforts in the cybersecurity domain which can fit in a comprehensive Research & Innovation Agenda,
- EC3 (European Cyber Crime Centre) created at Europol to be the focal point in the EU's fight against cybercrime, contributing to faster reactions in the event of online crimes,
- The StaySafeOnline service (to let users notify incidents and therefore better know cyber threats), implemented by the US NCSA (US National Cybersecurity Alliance), whose mission is to educate and therefore empower a digital society to use the Internet safely and securely at home,

work, and school, protecting the technology individuals use, the networks they connect to, and our shared digital assets,

- The Hackmageddon.com service to collect security incidents (on a voluntary basis only) and provide a picture of cyber-crime, hacktivism, cyber warfare and cyber espionage,
- ETSI ISG ISI (Industry Specification Group Information Security Indicators), a recent initiative with the creation during the autumn of 2011 of a dedicated standardization unit,
- R2GS (Club de Reflexion et de Recherche en Gestion Operationnelle de la Sécurité), a bottom up initiative of IT Security executives from large international end user organisations,
- ISACA Cybersecurity based upon COBIT and RiskIT globally used IT Security and Audit frameworks,
- STIX – TAXI, an initiative by the US Department of Homeland Security providing a technical framework allowing to standardize information exchange on vulnerabilities.

The ETSI ISG ISI initiative has been launched with the goal of meeting the abovementioned issues and challenges.

The 1st ISG ISI specifications have been published in 2013 (GS ISI-002 on Event model, GS ISI-001-1 and GS ISI-002 on Indicators, GS ISI-004 on Security incident detection implementation)⁹³, and they are now being used by some 25 big organizations and companies in Europe belonging to all industry sectors, especially those gathered through the network of Club R2GS associations (France, UK, Germany, Italy and Luxemburg), user communities specializing in Cyber Defence and SIEM (Security Information and Event Management).

The ISG ISI unit has also tied close relations with ISO JTC1 SC27 and ITU-T SG17 Q4 (Cybersecurity) through official liaisons; and the standardization world community agree that an important gap in this field is being filled by these new up-and-coming standards.

Several years of European experience with such approaches around information security indicators have proven to:

- Speed up progress in Cybersecurity through seriousness and alignment with management concerns:
 - Government Auditors – Enhanced level of assurance
 - Business executives – Better awareness of major IT risks and stakes
 - IT Operations and Production executives – Streamline OSM operations by maximizing the value of detection tools and teams
 - IT Engineering executives – RFP for SIEM or VDS tools
 - General management and CISO – Measure accurately improvement of user healthy computer behaviours in a threatening IT context
 - Human resources and management – Measure company loyalty

⁹³ Wikipedia entry on Information Security Indicators:
https://en.wikipedia.org/wiki/Information_security_indicators

- Stimulate exchanges within the profession (further to the ones found in existing Cybersecurity communities):
 - Collect and share experience on monitoring methods/use cases for major types of incidents/vulnerabilities/nonconformities
 - Make it easier to notify authorities

E.6.4 Required enabling technologies / capabilities

Given the current situation and the stakes explained above, to really measure and benchmark the actual effectiveness of organizations' security posture (tools, processes and teams) requires a comprehensive measurement system (and associated detection and monitoring tools) stemming from a relevant selection of controls and associated types of security incidents, vulnerabilities and nonconformities.

Providing the above services requires the following technologies and capabilities:

- Appropriate and standardized reference frameworks on this matter (top-down approach) to fill main gaps in technology (such as ETSI GS ISI-00x)
- Advanced security incident detection (to better monitor stealthy incidents such as APT, Web site intrusion, unauthorized access to resources...)
- Collection and working out by independent organisations of trustworthy state-of-the-art statistical figures on cyber threats and internal behaviours

E.6.5 Assumptions/Dependencies

It is assumed that security software vendors and security system integrators will design and develop better products and systems, whose (prevention or detection) efficiency could be far easier assessed and measured (especially through common and shared test patterns together with state-of-the-art statistical figures).

A side effect of the new services provided could be the occurrence of a golden age in cybersecurity insurance coverage (still with teething problems today).

Appendix F Example research topics and value statements

This section outlines a selection high impact security research topics justified by value statements. Each research topic should describe a requirement for an 'artefact' (e.g. a service, capability, reference framework, technique, enabling technology, etc.) that will be valuable in multiple usage contexts envisaged for around 2025. They should not be proposals for specific implementations of the artefacts. They should reference applicable use cases from the previous step in the methodology or other stages.

They topics are grouped according to a number of major categories of artefact we have identified.

- Security services and capabilities
- Trusted and resilient infrastructure
- Secure software/systems engineering methods and tools
- Security management solutions

While we do contend that the topics described are potentially 'high impact', they should be regarded as examples that have come up in the course of the study and not as an exhaustive list. The current topic descriptions are few in number, vary considerably in maturity, and have not been evaluated critically and ranked by the group as would normally be done in applying the methodology.

F.1 Security services and capabilities

F.1.1 Trusted Identity Service

The target market: service providers (that pay to Identity providers (IdP)) and end-users (that are usually not paying to IdP, at least not in the beginning)

Example case: incentivize use of privacy-preserving and/or enhancing "trusted identity" solution through government subsidy or zero cost for service providers in the first 5 years, in order to build "critical mass"

Value proposition: Research landscape deliverables list the following research challenges in this area: anonymous credentials, semantic and context based policies, etc. However, it is important to map these challenges to the specific value propositions. Context based security is, for example, very important with the increasing mobile access to the cloud, and it increases assurance level. However, inclusion of context parameters (e.g. location) in authentication process also has negative impacts on privacy. Measuring privacy is almost impossible, so how do we compare privacy levels of different trusted identity services? Should level of assurance (LoA) also include privacy parameters?

The clear value proposition, based on real figures and not assumptions, might be missing (e.g. privacy increases end user trust, as witnessed by x % increase in the uptake of privacy aware storage systems).

This section discusses cost benefit issues related to the topic of "trusted identity" interpreted broadly, and including the privacy domain (although privacy enhancing

technologies such as dashboards, for example, are not necessarily linked to identity management solutions).

Several identity and privacy initiatives have failed in the market in recent years. These include, for example, advanced electronic signatures whose market failure can be explained by a prioritisation on formal models valuing formal security guarantees and even pure complexity over practical relevance. More recently, marketing and economics research has collected a significant amount of facts and data about human behaviour with regard to factors such as use of online identity as well as diffusion of innovative systems and results which at times contradict the conjectures applied in the ICT security research domain.

The market for online trusted identities is slightly different than the rest of ICT security markets since it involves three parties: the identity provider (IdP), the service provider (SP, sometimes called the relying party) and the user, who can be a citizen, an employee or a legal entity. So in the trusted identity space market failure or success depends on service providers. The IdP will adopt results if the SP is willing to use the IdP. Therefore SP adoption is crucial. On the other hand, until a critical mass of users subscribe to the IdP, service providers' motivation to implement support for a specific IdP is quite minimal. Similar types of markets are payment networks or application ecosystems (e.g. the more developers that make applications for Android, the more users will adopt this operating system, and the other way round).

One of the predominant ideas in the recent EU research projects has been that privacy enhancing or privacy preserving features would foster market adoption of new user-centric identity solutions; this hypothesis has proved to be wrong, at least for the moment. One of the key requirements of truly privacy-enhancing identity systems, unlinkability, was achieved through the results of the Prime and Primelife projects through cryptographic mechanisms. This was integrated in Idemix, and announced by IBM as a "key market differentiator"⁹⁴, but wide uptake was still missing.

Recent surveys and experiments have explored individual privacy attitudes and uncovered a dichotomy between stated attitudes and actual behaviour. *This dichotomy, as well as the nature of e-ID market (service providers might prefer e-ID provider that shares more user attributes with them, not less) is probably the main reason for relative market failure.*

Meanwhile, simple and scalable lightweight protocols have achieved a rather wide market adoption. eID providers such as GoogleID or FacebookID are now quite commonly used by e-service providers. Adaptation of EU research projects to the new "landscape" has been slow, partly because of the nature and structure of IP or STREP research projects (some "sprints" in Trust in Digital Life" reacted more rapidly, for example), and partly due to the habit that only "hard" problems should be investigated including heavy protocols or high level of assurance. "Frugal" innovation is often missing. Both OpenID and OAuth (which was a protocol started by Twitter and developed almost at the same time and at the same speed as

⁹⁴ IBM Zurich Identity Governance research web page <http://www.zurich.ibm.com/idemix/>

OpenID), were started with a view on simplicity and in a certain sense exemplify the conflict between the cyber and enterprise cultures, where the SAML protocol would be a typical representative of “enterprise way” meaning complex, heavy protocol. But this is how “cyber” works: winners emerge not because they are the most secure.

Unlike OpenID based schemes and trust frameworks, the government based e-ID schemes sometimes include higher levels of assurance. It remains to be seen if policy instruments, such as eIDAS regulation, or results of e.g. STORK projects, will increase the market adoption of government issued online identities in a cross-border context.

A more recent trends and sub-segments corresponds to variations of federated identity management solutions, including (aggregated) attribute based access control, to the cloud-based service provision (IdaaS, AtaaS etc). Here, there is a waste know-how in Europe coming e.g. from educational eID federations. The actual research should build upon these existing schemes rather than reinventing the wheel.

F.2 Trusted and resilient infrastructure

F.2.1 Trusted Service Infrastructure

The target market: Large enterprises that have to optimise or migrate their IT to SOA based environments

Example case: Use decomposition into services as an opportunity to enforce or monitor security at fine-grain level

Value proposition: The research landscape deliverable is addressing several challenges in software and hardware infrastructures, for example decomposition of high level requirements stemming from legal or other compliance documents. There is no doubt that service orientation and the decoupling of applications presents a new opportunity to place security control probes in more places “inside” applications and to get more data from different layers. This control granularity has to be correctly translated into the value proposition, but the quantitative data about the cost of non-compliance has to be collected.

At the beginning of FP7, back in 2007, all major industry players identified the adoption of *Service Oriented Business Models* as a fundamental shift necessary to change the European economy into “*the world’s most dynamic and competitive knowledge-based society*”. This paradigm shift manifests itself by the “*evolution of business models from the sale of products to the provision of electronic services*”, where services are seen as utilities that can be used but that are not owned by users. Since then this shift affected all research areas and layers, from software to the network. However, cost benefit analyses previously done for migration towards SOA-based systems apparently made several wrong assumptions, since the adoption of these solutions was slower than expected.

NIS is following a convergent trend, for example by integrating formerly the separate network security, device security, software service security etc. The new generation infrastructures are being developed in cross-organizational ecosystems,

requiring new economic models, similar to those used e.g. in cloud computing (economy of scale). Increased organizational complexity is also making cost benefit analysis difficult due to the requirement that security should be mapped into high-level business goals as well as changes in organizational structures, individual work, and system development. Increasing adaptivity is another trend that is difficult to quantify when it comes to trusted infrastructures. We plan to focus therefore on e.g. assurance, evaluation and certification procedures that would lead to a faster adoption of the above mentioned service based infrastructures and paradigms.

F.2.2 Low-cost Security for Internet-of-Things Infrastructures (Matthias)

Research Topics:

- Lightweight HW support for secure sensors / IoT
- Scalable security protocols (for billions of devices)
- Distributed / decentralized

F.3 Secure Engineering (Tools and Methodologies)

F.3.1 Risk-driven secure engineering of critical enterprise systems

The target market: Enterprises that have to build critical systems

Risk assessment, management or requirements elicitation are common activities that apply to any security area. The quantifiable metrics that exist can be reused in cost benefit analysis. They provide a foundation for assessing the level of risk to which an organization is exposed (risk assessment), while the possibility of enforcement provides a means of mitigation by taking corrective action when the monitoring infrastructure has detected that something has gone wrong, or if it is likely that something will go wrong. However, risk assessment can be done at different stages during the software or system development, or can serve for comparative analysis.

Cost efficient engineering tools and methods that link with the existing practices in industry (e.g. UML) are increasingly available.

Value proposition: Research landscape mentions several techniques (e.g. early assurance) and issues (e.g. risk aggregation, cost) that are linked to this topic. As usual, the value is more security (higher assurance) with less money, so the argumentation should explore historic data that proves e.g. why early assurance is more cost-effective than late assurance, or why risk aggregation becomes compulsory to maintain the same level of security.

F.4 Security management solutions

F.4.1 Managed operational security for SMEs

The target market: SMEs that do not have their own network and security management staff

Here we could include all NIS areas where security is performed on an “operational” daily basis, from log collection and auditing to firewall and end-point

security. The trend of outsourcing started to cover the needs of both threat management, and as well as compliance. In 2010, the SIEM market reached 987 M dollars with annual growth of 15%, for example.

Value proposition: Research challenges in the other WG3 deliverable mention audit and monitoring tools, with few challenges that have been identified, although these are not specific for a single type of user. In fact, research advances are focused on highly sophisticated tools that need to be customized. The configuration management and assurance chapter in the WG3 “research landscape” deliverable, has made similar observations. The most obvious value proposition is cost reduction and the main candidates are technologies that include some form of self-adaptation and/or automation. For this reason it can be argued that the main innovation opportunities are in the application of modern architectural paradigms (e.g. use of event driven middleware, real time streaming processing etc.) to the security domain.

F.4.2 Quantitative Benchmarking of IT Security Controls

Given the current situation and the stakes explained in section E.6, to really measure and benchmark the actual effectiveness of organizations’ various security tools, processes and teams requires a comprehensive measurement system (and associated detection and monitoring tools) stemming from a relevant selection of controls and associated types of security incidents, vulnerabilities and nonconformities ; these must be based on appropriate and standardized reference frameworks.

The related possible (technical or not) research topics are the following:

- Advanced security incident detection (to better monitor stealthy incidents such as APT, Web site intrusion, unauthorized access to resources...)
- Cash in on the new ETSI GS ISI-00x standards on this matter (top-down approach) to fill main gaps in technology
- How to use state-of-the-art statistical figures on cyber threats to help insurance companies work out better and more accurate cyber coverage models and provide organizations with better products
- With the new wave of European and local country-specific regulations (upcoming European NIS and privacy directives) obliging organizations and companies (critical infrastructure and some other specific industry sectors) to notify security incidents to local authorities, how to classify clearly incidents and get a unique consolidated overview on them in each country and possibly across Europe

Such research initiatives (based on the approach explained in section E.6) could result in and stimulate:

- Security software vendors and security system integrators in designing and developing better products and systems, whose (prevention or detection) efficiency could be far easier assessed and measured (especially through common and shared test patterns),
- Organizations in better protecting themselves and in demonstrating tangible results,

- The profession in organizing the collection and the working out of more neutral and more dependable state-of-the-art statistical figures regarding main types of threats and weaknesses,
- The occurrence of a golden age in cybersecurity insurance coverage (still with teething problems today).