Be Wiser

Building Enterprises – Wireless and Internet Security in European Regions

Joint Action Plan Implementation

Measure A.3 - Ensure that ICT Security competences are provided to meet the needs and requirements of industry through Education & Training

A.3.1 (a) - ICT Security Skills Gap Analysis

Authors: Marianne Baumberger (inno),

Marc Pattinson (inno)

October 2015

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 319907

Table of Contents

1 Preface

"Building Enterprises – Wireless and Internet Security in European Regions" (Be Wiser) is an FP7 Region of Knowledge project.

Be Wiser Goals

- Helping companies become more competitive by enhancing access to research excellence, funding mechanisms and innovation through the improved interconnection of the actors in the field of Wireless and Internet Security ;
- Promoting the collaboration, exchange and dissemination of policy initiatives and best industry and policy practices at European level and beyond;
- Sharing knowledge between the different regions through inter-clustering;
- Developing targeted actions for cluster actors especially for SMEs (via support to open innovation, commercialisation, internationalisation and technology partnering);
- Implementing targeted internationalisation strategies and pilot actions to demonstrate their feasibility and impacts;
- Preparing Be Wiser clusters' members to exploit opportunities offered by EU-framework programmes such as H2020 and COSME.

Be Wiser Partners

The Be Wiser Consortium partners consist of seven ICT Triple Helix Clusters (THCs), drawn from different EU members states, namely:

- Systematic – Lead partner, and the Paris Region (France) ICT Triple Helix cluster
- Cork, Ireland – it@cork with its business membership plus relationships with the Cork Institute of Technology (including the Nimbus Centre) and Cork County Council, form the Irish Triple Helix cluster.
- Momentum, Invest NI and CSIT in Queens University combine to form the Northern Ireland Triple Helix Cluster
- CyberForum Germany – the Baden-Württemberg (Germany) ICT Triple Helix cluster
- Eurecat – the Catalonia (Spain) ICT Triple Helix cluster
- ICT Technology Network – the Slovenian ICT Triple Helix cluster
- Cyprus Computer Society (CCS) – a developing ICT Triple Helix cluster (Cyprus)

THCs support and animate a network of businesses, regional centres of research and technology, and public authorities responsible for investment in economic development. These clusters share a common objective of stimulating ICT and Wireless and Internet Security innovation, but operate in different ways, bringing together different strengths and expertise. Through this project, the clusters can offer a greater breadth of competence to the marketplace and can exchange successful practices. They can also achieve a critical mass to attract additional ICT clusters into the network. The internationalisation aspect of the project will identify links with expert clusters which are already in place, with the goal of further developing these linkages during the Be Wiser project. In addition to the Be Wiser technical THCs, the Inno Group provides benchmarking analysis support.

Be Wiser Joint Action Plan (JAP)

The Joint Action Plan (or JAP) is the centrepiece of Be Wiser project. In it Be Wiser partners set out actions which they agree to carry out in partnership, during the time span of the project and beyond. The JAP has been developed through a highly iterative process within each of the partner regions.

The JAP identifies key objectives:

- Objective A: Raise awareness and improve cybersecurity practice of citizens, and fill gaps relating to the cybersecurity skills needs of industry.
- Objective B: Ensure that the market requirements and business needs of the ICT sector are addressed through (i) the facilitation and development of technological and business relationships between actors associated with Be Wiser clusters, and (ii) developing & influencing ICT policy related to security.
- Objective C: Support the development of cybersecurity RDI initiatives, and facilitate SME and large enterprise access to RDI funding.
- Objective D: Strengthen the governance and operation of clusters through mentoring, staff exchange and cluster matchmaking.

For each objectives, the JAP specifies important actions and assigns responsibilities for delivering those actions. For each action in the JAP, three or more Be Wiser consortium partners agree to collaborate in order to achieve specific outcomes which will help to fulfil Be Wiser goals. The JAP sets out the actions to be undertaken, the partners who will collaborate in each action, the timeframe, the sources of finance which the action will draw upon, the likely impact of each action, and measures that will be used to judge the level of success of the action.

While some goals have a horizon which stretches beyond the boundary of Be Wiser project, other goals provide a blueprint for action by Be Wiser consortium members from the date the JAP is signed until the project's conclusion in June 2016. It is intended that the JAP will support Regional Innovation Smart Specialisation Strategies (RIS3) of partner regions, and identify further research and product opportunities as part of their broader economic development strategies.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 319907

2 Introduction to the Measure A.3 - Ensure that ICT Security competences are provided to meet the needs and requirements of industry through Education & Training.

The measure A.3 of the JAP is part of objective A: **Raise awareness and improve cybersecurity practice of citizens, and fill gaps relating to the cybersecurity skills needs of industry.**

Indeed, the Global Information Workforce Study found an ever widening gap between the supply of qualified information security professionals and the demand for skilled workers to secure critical information and the cyber world. The study found that the workforce will grow at a compound annual growth rate of 11.3% globally up to 2017, calling for an additional 2 million new workers.

Cybersecurity has become an increasingly important aspect of public policy as internet traffic increases and mounting cyber-threats affect the operation of governments and businesses as well as the everyday life of citizens. Cybersecurity policy-making is at a turning point, becoming a national policy priority with explicit strategies in several countries.

Understanding and interacting within a secure and trustworthy digital environment is of benefit to all European citizens, and in this regard a plan must be articulated to educate and develop awareness of safe practices when online at an early age. Providing awareness and training for citizens may also help citizens to engage with technology and use it to their advantage earlier, with a potential effect of sparking interest in ICT and cybersecurity related careers.

Thus, 3 measures will be proposed under the Objective A:

- Measure A.1: Increase awareness of the importance of a secure and trustworthy digital environment for the benefit of all EU citizens.
- Measure A.2: Develop channels at pre-tertiary education levels to enrich cybersecurity awareness.
- **Measure A.3: Ensure that ICT Security competences are provided to meet the needs and requirements of industry through Education & Training.**

Even though the availability of high-level ICT security skills would significantly contribute in leveraging the economic growth of companies, still there is a lack of ICT security skills in Europe. As described below, there is an ever widening gap between the supply of qualified information security professionals and the demand for skilled workers to secure critical information and the cyber world (an additional 2 million new workers required byl 2017). As a result, several hundred thousand ICT-related job vacancies remain unfulfilled. The educational sector and industry have to closely collaborate to satisfy security demands in this rapidly changing field. Thus, the goal of the action A.3 is to identify measures that the educational sector and the industrial sector could take to provide the required ICT security competences.

To reach this objective, BeWISER partners will work together through a three steps process:

- Identify missing ICT security competences for the industry at national/regional level, and highlight recurring shortcomings across Be Wiser regions
- Create a directory of ICT security courses offered in each Be Wiser partner region to include: Degree / Master courses and modules offered by HEIs and Training and Certification courses offered by professional associations/institutes and industry.
- Encourage engagement between HEIs and cybersecurity professionals from industry for course review and curriculum development.

The current document correspond to the first step: identify lacking ICT security competences for the industry at national/regional level, and highlight recurring shortcomings across Be Wiser regions.

The objective is not to conduct an in depth analysis of the ICT skill shortage issues in Europe but rather to identify the main trends, based on a literature review of existing reports/surveys on the ICT security competences in partner regions, the security skills and competences recommended by selected professional and other ICT related organisations, and the Be Wiser Roundtable Discussion Reports (deliverable D3.2).

3 Main trends related to security competences for the ICT industry

To become innovative and competitive, an economy needs a workforce with the relevant competences, in line with the market and sector trends. Today with the digital transformation, companies have to rapidly and efficiently design or adopt new technologies, and have to modify their way of doing business: ICT skills and competences are essential for driving innovation and business growth. And due to the digitalisation of the world, ICT skills are required both for ICT practitioner and for non-ICT occupations. Thus, ICT skills and competences are therefore a major policy concern in Europe to reach the Europe 2020 strategy and its objective of smart, sustainable and inclusive growth.

Regarding ICT practitioners, the top 10 IT skills in demand worldwide in 2015 are:

Figure 1 - Top 10 IT Skills in Demand for 2015 – Source: THOMAS WADLOW, chart produced by inno

Three listed skills are clearly and directly linked to security competences: cloud security, Ethical hacking, and Secure coding.

This outcome in itself is not surprising: in a world where the virtual world increasingly impacts the real world, our growing dependence on internet technologies and the interdependence between critical resources and infrastructures and connected technologies raise important security issues. Furthermore, the Global Risk 2014 report identifies cyber-attacks, infrastructure disruptions, and data loss (fraud, theft) as the three main technological risks faced by the world.

The **World Economic Forum** demonstrates also that organisations are faced with a growing volume of cyberattacks: in 2013, there was a 62% increase in the number of security breaches, and 2.5 billion records had been exposed in the last five years as a result of a breach.

IT Security skills are essential for Europe's economy, and the gap between the demands for trust, privacy, resilience and confidence of IT on the one hand, and the knowledge, skills and competences of the workforce on the other, must be understood and reduced.

According Alice Hill, managing director at Dice.com[1]: “every year the number of threats and the sophistication of those threats escalate. It's a battle that will only continue to increase, making cybersecurity positions a priority within organisations."

On one hand, organisations need to put in place effective policies that speak to corporate boards, managers and employees at all levels; and on other hand organisations need to have the staff who know how to use the existing tools (there are cyber intelligence tools capable of tracking and alerting on the latest vulnerabilities) and who really understand the threats and their consequences, especially responding to live-attacks in real world situations.

Additional evidence from a variety of sources shows an ongoing IT security skills challenge:

- According to the ISACA 2014 APT Survey, 62% of organisations have not increased security training in 2014 though, in direct contrast, the cost of breaches is thought to have doubled last year in the UK alone.
- According to NTT Group’s Global Threat Intelligence Report**,** 77% of organisations supported during incident response activities had no incident response plan in place.
- According to the Cisco 2014 Annual Security Report**,** approximatively 1 million of IT security jobs worldwide are unfilled.
- According to the UK’s National Audit Office, between 1998 and 2000, approximatively 70% fewer graduates attended courses in Europe that were core to entering IT professions. The result is a skills gap that may take generations to fill – 20 years.
- According to a 451 Research Q2 2015 study, based on responses from over 1,000 IT professionals, primarily in North America, Europe, the Middle East and Africa, security managers reported significant obstacles in implementing desired security projects due to lack of staff expertise (34.5%) and inadequate staffing (26.%). Given this challenge, only 24% of enterprises have 24×7 monitoring in place using internal resources.
- According to a Rand Corporation study, there are around 1,000 top-level cyber security experts globally for a need of 10,000 to 30,000.

Many studies conducted worldwide and at the European level demonstrate a clear lack of skilled security experts entering the market, and a dire lack of investment in training: all competent authorities agree that there is a major and growing IT security skills shortage that will impact on economic growth and the competiveness of European businesses.

[1] **Dice.com** is a career website based in Urbandale, Iowa. It serves information technology and engineering professionals. Dice.com typically has approximately 60,000 tech job listings. The website claims to have 3 million registered technology professionals and approximately 2 million unique visitors each month.

But, to be useful and of use to practitioners and those in a position to alter the situation , it is also important to know the exact skill sets that are in highest demand. The field of IT security is not monolithic, but it is made up of a variety of skill sets involving a combination of technical, planning, and managerial skills.

A classification of the IT security skills was developed at European level by the European Committee for Standardization with input from governments, organizations, and professionals across the EU. This system defines 23 job profiles under six areas of IT security: business management, technical management, design, development, service and operations, and support.

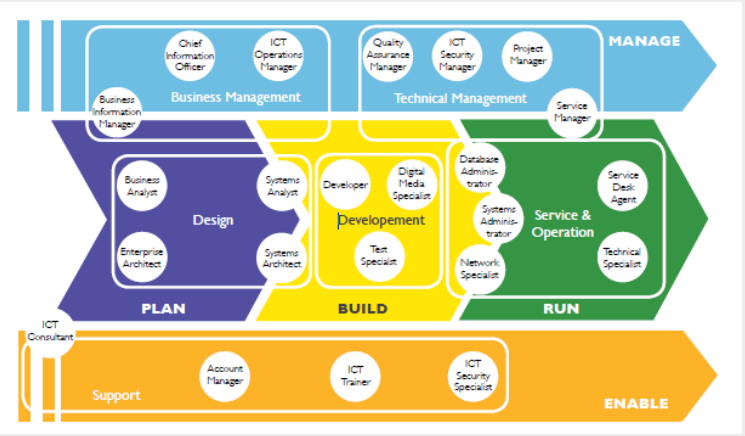

Figure 2 - The EU framework of IT security skills

These jobs also cluster into five segments, each driven by an action verb: plan, build, run, enable and manage. For each verb, required IT security abilities are defined :

Planning	The ability to implement security related aspects in system architecture, product or project planning. Knowledge of ICT solutions and understanding of security-related complications.
Building	The ability to deliver or purchase solutions that are secure and reliable. The ability to integrate security at the earliest possible phase of design and development. Addressing security implications in interplay between and integration of systems.
Running	Delivering secure software, infrastructure and services. A "security mind-set" needed by people undertaking daily execution of activities. Forming and spreading a security culture among users.
Enabling	The ability to formulate an organisation strategy, scope and culture for safety and security of information. Detecting and raising security issues in formulation or purchasing instances.
Managing	The ability to implement the strategy, scope and culture for security in the organisation. Manage security on a daily basis in accordance with business needs and developments.

Figure 3 - E-skills for IT security in different practitioners function – Source : e-skills for security report

The Global Information Workforce Study conducted an analysis to identify the skill sets most needed by organisations, amongst a list of 39 job categories, inspired from the European Union framework and the USA's National Initiative for Cybersecurity Education (NICE).

Results of the survey are summarised in the graph below.

- The skill set most in demand is **Security Analyst** who conducts the integration and testing, operation, and maintenance of systems security, with 47% of respondents naming this position as their top need.
- Three of the top ten job titles in demand are in **Security Engineering** (planning/design, applications, platform), indicating a growing understanding of the need to include security in the planning, design, and development of information security systems and processes, and in the development of new applications.

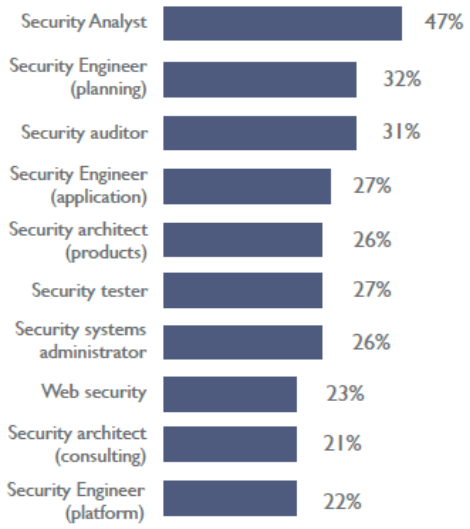

Figure 4 - Shortage by job titles (Top 10) - Source : Global Information Workforce Study

In addition, some specific trends have been highlighted according the sectors.

- For government (military and non-military positions) the rankings are nearly identical to those of the total sample, except for the need for **Forensic Analysts** that reach the top ten desired skills. Forensic Analysts collect, process, preserve, analyse, and present evidence to support network vulnerability mitigation and/or breach investigations. Compared with other industries, they also have greater need for Security Engineers (planning and design, and requirements), Security Systems Administrators, Security Testers, and Incident Handlers.
- Healthcare companies show a greater need for Incident Handlers and Web Security specialists.
- Information technology companies find higher-than-average demand for Security Engineers with application experience and management consultants in security.
- Telecom and media companies have greater need for Security Engineers in both planning and design, and platform development, as well as Security Architects with products/solution experience.

The career website Dice also conducted an analysis about the most in-demand IT security skills, with the following interesting results:

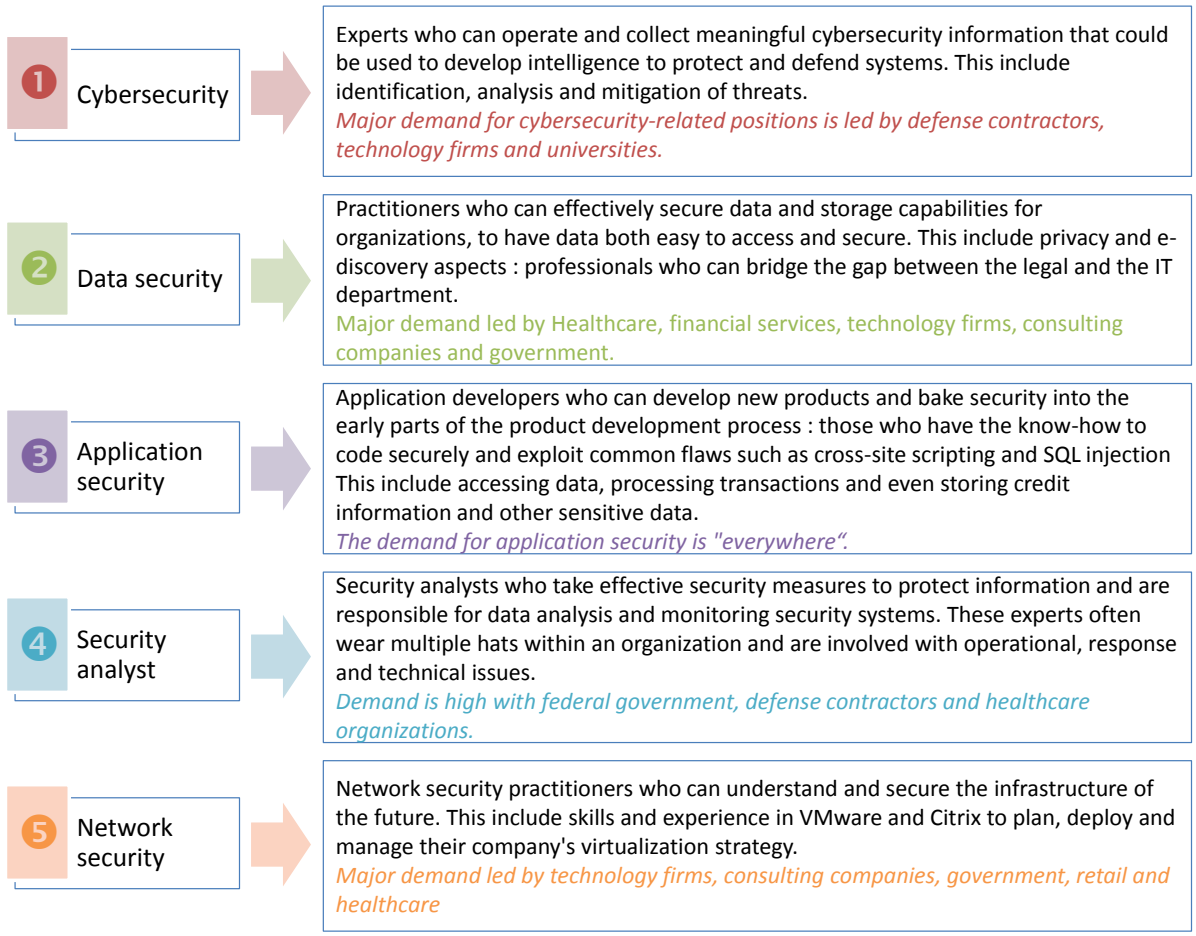

Figure 5 - 5 most in-demand IT security skills - Source: Dice, chart produced by inno

The results of such an analysis can be used to help define educational and training content. They can also help cyber security firms design service offers to meet the needs of other businesses. Triple helix cluster partners can also use these results to raise awareness of such studies and results with their members.

4 Focus on the BeWISER regions

The following sections provide a summary of the ICT Security Skills issues for the BeWiser regions.

4.1 Paris / Ile-de-France Region

While "standard" ICT competencies are rather easy to find, more specialised skills such as IT security skills are difficult to source and attract. This statement is explained by a combination of several causes:

- **Lack of current provision of skilled ICT security graduates and curriculum development.** In a general way, less young people are attracted by the ICT sector compared to the past. In addition, although the Ile-de-France region has a good training ecosystem related to the ICT domain (there are approximately 20.200 ICT students in the Ile de France region, distributed between 70 universities / schools), regarding the security domain, it is considered that **an insufficient number of new security engineers are trained to meet company needs**. On one hand, the educational offering in the domains of wireless and internet security is viewed as 'insufficient', 'too general' and not up to the standard required. On the other hand, students are not attracted by high tech specialised curriculums at a thematic Masters level and they prefer keeping more options open. It is worth noting the ANNSI (National Agency for Security of Information systems) initiative to improve IT security training in France and Ile-de-France : it conducted a mapping on the existing training offer (5 master degrees from Universities, 6 master degrees from Engineering School, 6 Engineering diplomas from Engineering School, 1 MBA from Engineering School identified in the region), and it has published in February 2014 a tender (CyberEdu) for creating higher education training modules in cybersecurity, that will certainly accelerate the development of training in this field. Public authorities are indeed well aware of this lack of competences and the weak offer in terms of training.

- **The attraction of skilled IT security talent problem.** Companies in the Ile-de-France region **are struggling to attract qualified people**. Numerous students and new graduates leave the region every year for the USA due to higher salaries and better funded research and working environment: better tax packages, more flexibility, faster growth prospects and attractive projects are other reasons cited. In addition mobility between research and business is not a common behaviour in France: researchers working in HEIs are not ready to move to enterprises, and companies have a preference for engineers rather than for doctoral students and doctors.

- **The ineffective Up-skilling & continuous professional development process.** In France employers have a legal right to offer CPD training (DIF- Droit Individuel à la Formation). However, it appears that this right is **complicated to implement in the case of very high skilled workers**, or in the case of career change, and ongoing training is often only related to generic subjects (e.g. English, management etc.). In addition, there are differences between large companies, able to provide internal training, and SMEs which have to externalise (and therefore find training in line with their needs), and which don't spend time and money for this (and in particular in times of economic crisis). From the government's perspective, a good initiative has recently been launched: ANSSI has developed a training centre in the security of information systems (CFSSI), in charge of the implementation of training sessions dedicated to the staff of the French administration and army.

- **Few partnerships exist between business and training providers.** Companies state that the existing trainings (initial and/or life-long learning perspective) do not always meet their needs, in the content and in the form (for example, the lengths of student and graduate internships is considered as not sufficient, under 6 months). To solve that, companies have to be genuine contributors to initial and CPD training: but in the real world, in general companies are passive in the definition and in the implementation of the training programmes, due to a lack of relationships and common work habits between companies and training providers. It follows that companies feel that it is easier and more relevant to train an employee directly, but as noted previously, internal training is basically only practical and feasible within big companies.
- **Few conversions of non ICT graduates from other sectors into IT security workforce.** Due to a global shortage in ICT security talents in parallel with unemployment in many other industry sectors, we must consider conversion of unemployed labour as a "massive" solution. But, besides the technical difficulty for reconversion (IT security is highly tech specialised sector), only a few candidates actually apply for conversion into the ICT and the IT security sector: conversion remains an individual decision, and there is a lack of information on jobs opportunities to the unemployed.

To reinforce the IT security skills in Paris / Ile-de-France region, several initiatives are being considered. Among them: develop awareness and motivation of students and for the unemployed about IT security opportunities, increase relationships between industry and educational and professional training to better adapt training programmes, develop new schemes for life-long learning and make them more accessible for SMES such as MOOCs.

4.2 Barcelona / Catalonia Region

Despite the economic crisis, the IT sector in Spain and in Catalonia is in good health, so for IT professionals it is not a big concern moving between regions or competencies to develop their career. In parallel Barcelona is an attractive location for IT professionals: the brand of the City draws people, and there is a good provision of IT skills in the region: Catalonia has a large pool of skilled and specialized people with more than **70 000 highly-trained ICT** professionals. However, even the IT and security sector faces problems through the lack of qualified people to fill vacant ICT and security roles.

- **The decline in the number of ICT graduates over the last number of years,** due to demographic reasons, loss of popularity amongst students in technical degrees and a perception that a significant amount of effort is required to be awarded a honours degree. Thus, significant demand for ICT graduates in the fields of system administration and applications development exists in Catalonia: enterprises are seeking more specialised practical skills to meet market needs, which can complement the high standard of theoretical education provided.

- **The lack of communication, interaction and understanding between industry, HEI, and students.** There is a lack of understanding by HEIs of the profile requirements and overall market demands. Furthermore, students only make contact with industry when they are almost finished their studies, or after completion. Finally, companies also have to provide technical training for staff to fill the gap between the technical skills required by the enterprise and university graduates.

- **The difficulty to adapt the educational offer to meet industry needs.** The regional diagnosis enabled the identification of only five specialized degrees on this domain (related to 1830 students

trained in ICT). In addition, lifelong learning of professionals to update their competencies is not very developed, and security is not an easy topic to find outside of specific university courses. This difficulty comes from the combination of 4 main factors: (i) Culture: there is a weak culture of training in Spain, and companies assume that professionals will update skills on their own; (ii) Time Limitations: the working day in Spain starts at 8:00 or 9:00am and finishes anywhere between 18:00 and 20:00, and this does not really allow time for evening courses or at least makes this possibility unattractive ; (iii) Academic Bureaucracy: a significant amount of bureaucracy exists into the process of developing academic courses; (iv) Format: current courses offered generally have a long duration e.g. part-time over 2 years, and there is a lack of industry input from the academic teaching perspective.

- **The bigger challenge of training for SMEs.** There is a difference between large companies, who have integrated training programme partnering with training centres or even considering in-house training, and SMEs, who find it difficult to train their workforce in regard to the lack of resources, expertise and co-ordination.

- **The low potential of conversion related to IT-security technical competences:** conversion requires a significant investment in time and money and there is a perception that only those with college degrees would be able to adapt to the knowledge requirements of the IT sector. An opportunity exists to convert incoming people not to pure IT professionals, but to the surrounding skillsets which complement the sector e.g. marketing, social media management, content management etc.

- **A big challenge for local IT start-ups.** Despite there is a lot of effort from the local agencies of the public sector to promote entrepreneurship and self-employment, the legal and bureaucratic framework for this new venture to develop is still complicated and suffers from a low pace to set in motion these initiatives. Also, in comparison to other European regions, tax burdens may be discouraging and also direct costs to maintain the activity (especially regarding the requirements for having own offices or a corporate location) may be a barrier to boost entrepreneurship

To reinforce the IT security skills in Barcelona / Catalonia region, several possible actions are open. Among them, specific effort must target the promotion and awareness initiatives of ICT and IT-security courses and programmes, and the merger of industry needs and opportunities and training offers. Clusters are well placed to develop and inform stakeholders of these needs. Many new and innovative tools could be put in place: students mentoring projects, online marketplace for companies to sponsor courses, live study programmes where students could try to provide solutions to real enterprise problems or R&D challenges, an observatory of alignment between offer and demand between teaching thematic and market demands…

4.3 Karlsruhe / Technologie Region Kalruhe (TRK)

Karlsruhe is one stronghold for the ICT sector in Germany. More than 4,200 ICT firms are located in the region, many of whom are SMEs. Firm are seeking growth, but are constrained by the difficulty to find suitably qualified employees. This situation is not specific to Karlsruhe, but due to the strong presence of ICT on the regional economy its effects are significant. SMEs are particularly constrained by skills shortage as they compete with large companies e.g. SAP, for qualified staff.

- **Mobility and attractiveness of ICT graduates and professionals.** Karlsruhe is home to an excellent education and vocational training system containing high-quality universities and HEIs. Significant expertise in ICT courses exists with more than 5.600 students enrolled annually related informatics and similar subjects. However, few stay in the region, many leave for more "attractive" regions like Munich or Berlin. Foreign students tend to leave when their studies are completed. Indeed, the attractiveness of a region depends not only on its job market situation (that is very good in the TRK region), but also on the housing situation (where significant shortages exist regionally) and the quality of life for younger people (e.g. nightlife, which is not comparable to Berlin or Munich) and for families (e.g. amount of available spaces in day-care centres). And for many skilled ICT employees, the quality of life is the second important factor (after the salary requirement) for a job decision. Thus, TRK does not find it easy to attract skilled ICT talents from other regions or countries: Karlsruhe has to compete with other, larger and/or more famous regions in Germany. But the city and the regional government are working strongly on this topic. Additionally, many of the successful and innovative ICT companies in TRK are SMEs: often they are not well-known by the public and/or potential applicants. There are examples of so-called SME hidden champions (e.g. WIBU Systems in the field of hardware security and software licensing).
- **Limited space for security in the IT training courses.** Some of the HEIs of the region offer single modules for IT security (basics, cryptography, encryption methods, digital signatures, public key infrastructure etc.) within the curricula of courses such as informatics, information engineering and industrial engineering. No specific course exists exclusively in "IT security" and no specific degree for citizens aspiring to become an "IT security manager". Internet and wireless security form part of the courses offered across HEIs in Karlsruhe. Participation in these modules is not mandatory for students (optional subject for a specialization in advanced study periods). However, since the break of the scandals involving the NSA and GCHQ, awareness of IT security has been raised exponentially in science and higher education on regional and national level. In the meantime, new lectures like "Selected chapters of cryptography", "Symmetrical cryptographic techniques", "Cryptographically voting procedures" or seminars with topics like "Advanced encryption techniques", "Cryptography in practice" or "Crypto-analysis" have been developed in order to face the challenge of the current IT security situation. When they finished their bachelor studies, students can decide to set a larger focus on the topic IT security on their way to a master degree. Furthermore, there are several private institutions for professional development offering IT security courses for both people with a degree in informatics or a similar subject and career changers or even for people without any study degree. Courses are offered for degrees like ISACA Certified Information Security Manager (CISM) or IT security manager according to ISO-27001. Even the Federal Office for Information Security offers courses which covers the so-called "IT-Grundschutz" (basic IT security). The regional special interest group "KA-IT-SI" (Karlsruhe IT-Security Initiativ) with 20 members from science and industry promotes the topic and creates awareness for IT security in industry, science and education.
- **The difficulty for SMEs relating to traineeship up-skilling and Continuous Professional Development (CPD).** Traineeship and CPD are a good ways for companies to have employees with the relevant competences, those meeting their industrial expectations. Despite the awareness about this necessity, start-ups and SMEs are often not able to offer traineeship or CPD. A major problem for SMEs to offer traineeship opportunities for students is the requirement of significant

time and other resources for this purpose: in many cases, apprenticeships are shared because young companies often don't have the resources to provide the entire apprenticeship. In addition, start-ups and SMEs are often not able to offer CPD to their employees for organisational and/or financial reasons. Several public funding programmes exist which support CPD in companies, but many start-ups and SMEs have a lack of awareness of these programmes and are not well versed in applying for funding in this regard.

- **The skills shortage of reconversion.** The regional ICT industry recognises the potential of specific groups (e.g. immigrants, older/retired workers, career changers, women - especially after maternity, career breaks or college dropouts) to fight the ICT and IT-security skills shortage. At present, several initiatives have been started for reskilling/integration and conversion of these groups of persons to the ICT workforce. Nevertheless, a skills shortage exists, as not enough people are motivated to reskill, and furthermore, in some instances the offered courses are not appropriate for industry requirements (e.g. not enough practical elements). People tend to take courses in line with their interests and background knowledge. However, the resulting degrees are often not required by the ICT sector (e.g. many web designers vs. less Java developers).

To reinforce the IT security skills in Karlsruhe / TRK region, several possible actions are open. Among them, are specific efforts for increasing the attractiveness of the region (working on marketing but also on related aspects such as housing, quality of life …) and of the ICT and IT security sector to attract a variety of group such as immigrants, older/retirer workers, students, and new graduates… Reinforce the proximity between HEI and ICT industry is also a key aspect to foster traineeships, CPD, and the emergence of a new curriculum in line with the requirements of ICT companies: fiscal and/or financial incentives could help (especially SMEs). Finally, IT security should become an integral part of the curriculum in all informatics related courses.

4.4 Cork / South West Region

Education and Human resources in ICT are well developed in the County: within the region education in ICT related fields represents some 2 090 students, of which some 50% are deemed to have followed training on wireless and internet security as part of their studies. Education in ICT is mostly done through universities while education in security is mostly private (essentially performed by big companies). With regard to the weaknesses in the region, there is dependency by Cork ICT firms on recruiting IT and software professionals, including data analytic skills, from abroad, as the required professionals and experience are lacking locally. Many of the MNCs based in Cork require professionals IT and language skills to work in their global service and client centres. At a national level, Ireland has a need for more IT-security skills, in particular in **storage and security** (there is a requirement for top level PhD researchers in ICT security, and Storage & networking. Only a small number of these specialised positions are available, however companies such as EMC^2 have had to look overseas to fill these positions.

- **Adapt the current provision of ICT security education: provide professional experience for ICT graduates.** Many MNCs and SMEs require ICT professionals with a minimum of 3 years experience and not necessarily graduates. Thus the issue for employers and graduates in the region is to ensure that new graduates can acquire the necessary experience and training. Industry suggests that practical skills are not given sufficient credit in universities; instead the focus and acclaim is on research. However the perception in industry is that it is better to hire people with practical

experience rather than theoretical experience only. Developing work placements and traineeships offer many opportunities for putting classroom learning into practice, and afford many opportunities for informal learning in the workplace. But organising successful work placements requires considerable resources from both the HEIs and employers. This represents a barrier to SMEs taking on work placements due to the time and costs in organising them.

- **Mismatch between 3rd-Level Courses and Industry requirements.** There is currently no undergraduate course on internet security provided in the region. There is also a skills shortage in wireless security and wireless technology and in particular radio and radar design. HEIs have difficulty providing the number of graduates that industry needs, in a timely manner. By the time students complete a 4 year course and acquire 2 years' experience, technology trends are already changing. The solution requires courses to become more responsive and flexible. Higher Diploma courses are acknowledged as being responsive to industry and beneficial in reskilling students with primary degrees in new areas with skill demands. Academia is too focused on technical skills and it needs to produce people who have a more rounded education which includes interpersonal and social skills and emotional intelligence.
- **Employment Retention for SMEs.** There is a difficulty in retaining employees for Start-ups and SMEs: after graduates join a small company and gain experience, they are often poached by larger companies.
- **Attractiveness of ICT talents**. The tech sector in Dublin is widely known throughout Europe and is the European HQs for companies such as Twitter, Google, Microsoft and Facebook. Cork is not as widely known as a tech hub which reduces inward skilled migration increasing the local skills gap. Technical professionals are a highly mobile group, and the private sector is working on the attraction of a significant number of technical and multi-lingual professionals through support for Make IT in Cork, a regional branding initiative (online platform) to attract professional migrants. www.makeitincork.com
- **Lack of time and resources for up-skilling and CPD in Start-ups and SMEs.** Despite the number of up-skilling and Continuous Professional Development (CPD) courses provided in the region through HEIs (the technology centres in Tyndall (UCC) and NIMBUS (CIT) provide training to ICT companies: UCC and CIT provide online degree courses in Cloud, Big Data etc.) and Skillnets[2] (IT@Cork, Cork Chamber etc.), up-skilling and CPD is considered a critical issue by SMEs. Academia acknowledges that they lack sufficient funding and resourcing to meet the up-skilling needs of industry. Possibilities for career development are said to be too management focused at present, and need to be expanded horizontally with financial reward given for raising technical and professional skills to higher levels.
- **Primary and Secondary Level Support.** Computer Science needs to be taught at primary and secondary level. Teachers (especially at primary level) need the skills to teach different levels of computer science modules and to meet changing curriculum needs. There is a Government failure to promote ICT & Science as a career option for 2nd level education students. Work experience

[2] Skillnets training networks are groups of private sector companies in the same sector and/or region that have come together to carry out state subsidised training activities that may not be possible on their own

during transition year should be more practical and beneficial. It is an opportunity to introduce students to the world of technology.

To improve IT security skills in Cork / South West region, several lines of actions are open. Among them are initiatives to support graduates to have professional experience (facilitate and structured work placement, develop joint programmes with ICT companies offering business modules, etc.), and to provide more flexible training for degree courses and up-skilling courses to react to industry needs (improve links with industry: there is a requirement for more and wider inputs from industry).

4.5 Belfast / Northern Ireland Region

There are **approximately 3 000 students in Computer Science, with an additional 3 000 in Engineering and Technology disciplines. 3 universities** have ICT related departments/degrees, of which 2 (Queen's University, University of Ulster) have also security related departments/degrees (one university clearly provides Masters in security). In addition to that, **6 Northern Ireland schools** have both ICT and security related departments/degrees.

Most of the challenges faced by Ireland are also faced by Northern Ireland Region: to find ICT professionals with a minimum of 3 years' experience and not necessarily graduates (and the need to develop work placements and traineeships), to retain employees for Start-ups and SMEs because graduates have a preference for larger companies, the lack of attractiveness of the region due to its peripherality (there is a net outflow of skills from the region) ; the mismatch between 3rd-Level Courses and Industry requirements ; and the need for primary and secondary level support.

Specificities of Northern Ireland are:

- **Lack of connection between skills providers and industry**, despite the existence of Industry Liaison Panels tasked with bringing together the needs of industry within the capabilities and plans of the education sector. One of the significant initiatives in training is the MSc in cybersecurity launched in September 2014 by QUB-CSIT. A key differentiator of this MSc programme is the opportunity to closely engage with CSIT industry partners. This includes the facilitation of industrial internships with leading security professionals, as well as other commercially specified and co-supervised projects. Invited seminars and special guest lecturers from influential industry and academic leaders offer students a chance to engage with those at the pinnacle of the cyber security profession.
- **Lack of Premium Level PhD Researchers:** there is a requirement for top level PhD researchers, particularly in ICT security, in storage and in networking.
- **Lack of ICT conversion:** there is a lack of awareness on the broad range of employment within ICT from programming to sales to HR; and ICT conversion courses in their current form are too broad and need to be categorised into different ICT disciplines.

To improve IT security skills in Northern Ireland, several lines of actions are open. Among them are to adapt the UK national Higher Apprenticeship for the regional development; to reinforce linkage between companies which are up-skilling and HEIs and bodies providing up-skilling, so they can tailor courses to meet companies' requirements ; to provide entry level ICT courses in specific areas for those at risk of long-term unemployment; and to develop National and regional Government

initiatives giving children a fun way to develop ICT programs, and encourage more female students to consider a career in IT.

4.6 Slovenia

According to recent study and expert opinion, there is still a shortage of ICT practitioners in the country. And it is expected that, as soon as the economic situation improves, demand for ICT practitioners will jump up. Thus, there is not only a shortage of ICT experts for the existing profiles but also a great need for new profiles, such as big data analysts, multimedia, new industries, etc. ICT is becoming more and more an interdisciplinary profession and it is important to integrate it into all industries. Slovenia has a share of ICT specialists in the workforce of 2.6%, just below the EU average, and Slovenia compares favourably on the % of STEM (Science, Technology, Engineering and Mathematics) graduates, with 1.9% of Slovenians aged 20-29 years old holding a STEM degree. There are opportunities to meet ICT industry requirements:

- **The gap between the theoretical knowledge of ICT graduates and the experience companies require from their employees**. 3 universities and 15 schools have ICT related departments/degrees, representing 20,545 students. These 3 universities and 5 of these schools have degrees/departments in security, but regional stakeholders consider that there is not enough focus on wireless and internet security in general, and there is a lack of courses developed around internet security. Critics also complain that the Slovenian educational system provides students with too much theory and not enough practice.
- **Reverse the brain drain**. According to Digital Agenda for Europe data, there is a surplus of skilled ICT experts in Slovenia. The main challenge for Slovenia will therefore be how to stop brain drain, rather than how to attract foreign ICT experts. Otherwise, Slovenia as a starting point is an attractive destination for experts from Serbia (and other countries of former Yugoslavia) wishing to work in the Schengen area. With the accession of Serbia to the EU, the pull factor will be lost. If it is easier to attract experts to work for academic institutions, it is almost impossible to attract experts to work for companies due to large administrative obstacles in granting work permits (Ministry of Economic Development and Technology).
- **The failures of the apprentice system**. The main issue emphasized was that students who start working during their studies usually experience serious delays in graduation or they don't graduate. Many smaller companies see students only as a resource and are not interested in their long-term education and skillsdevelopment. The apprentice system is very complex from an administrative perspective, therefore, companies rarely decide to make use of it. Another issue relates to the time it takes to introduce students to the work systems of individual companies.
- **The under-development of life-long learning.** There are a number of experienced ICT professionals who work on specific technologies for a long period of time, and have limited time for up-skilling. A significant challenge relates to how such staff upgrade their knowledge and allow them the opportunity to compete in the market with newly adopted skills. Only a small number of up-skilling and professional development courses are available in Slovenia because the market is small. It is very important that industry experts have the opportunity to get up to date expertise from abroad. According to the policy representatives it is the responsibility of the industry to financially enable staff mobility.

To reinforce the IT security skills in Slovenia, several lines of actions are open. Among them are the removal of some administrative / legal obstacles (such as financial incentives for employment of new graduates, or administrative procedure for work permits for foreign workers), particular attention to faster employment of new graduates by the ICT industry, and awareness about the opportunities of internationalisation (attend courses abroad when relevant up-skilling courses are not available in Slovenia).

4.7 Cyprus

Eurostat reports that there are a large number of ICT jobs vacant throughout Europe. However, this is not the case in Cyprus where the unemployment rate among young ICT graduates is high compared to three years ago. There is currently a surplus of qualified ICT graduates which forces many to seek employment opportunities abroad or, those who study abroad, to stay and work abroad. In addition, industry representatives believe that ICT graduates suffer from a lack of practical experience and business mind-set among academics, and the title "Qualified" is usually coupled with unreal remuneration expectations (for Cyprus companies) from candidates.

- **Mismatch between curricula and ICT industry needs.** Cyprus hosts 8 Universities with ICT related departments and degrees: more than 1800 students follow ICT related courses offered by the 5 private and the 3 public Universities. Regional ICT companies stated that the curricula of local universities in this field do not currently meet the needs of the ICT industry and that most ICT related university programmes are still too theoretical. They attributed this misalignment of ICT curricula and the ICT industry skills needs to a number of reasons, as stated below: (i) there is a gap between the educational and industrial sectors and they don't align together; (ii) Universities do not update their curricula frequently enough to follow the rapid changes in ICT; (iii) the Universities focus too much on theory; and (iv) there may be a lack and delay in integrating new technologies into the curricula. As regards IT Security curricula specifically, up to two years ago no such university programmes existed: however, some of ICT curricula offer courses in the security area. In the last few years one of the Universities offers a graduate degree in Cybersecurity and two of then offers concentrations in the security area for the graduate degree. In addition, more courses have been offered at the undergraduate level. Regional ICT companies call for their timely design and introduction both at undergraduate and graduate levels.
- **The employment paradox**. Due to the economic situation in Cyprus, ICT graduates know an high unemployment rate, and a lot of the local ICT professionals can't get the experience requested by such employers due to the lack of companies that can offer that kind of experience: unemployment rates is a factor contributing towards lack of professional experience of ICT graduates. Thus, a number of local ICT companies attempt to attract experienced ICT professionals from other countries, but this is not a large number. Many offshore companies operating from Cyprus also employ foreign ICT personnel, especially ICT professionals from the Russian Federation and the old Eastern European countries. In parallel, skilled ICT talent (qualified graduates) and experienced ICT professionals from Cyprus prefer to emigrate for improved employment prospects: other EU regions and countries can offer higher wages to attract them. These skills are in demand across Europe and it is of importance to the Cyprus ICT industry that it retains these skilled and experienced professionals.

- **The lack of formal work placement or apprenticeship programmes between industry and academia**. Universities are looking for opportunities for student placements and apprentice internships, but there is a lack of internship availability and/or interest from the industrial sector, and no formal programmes are in place: usually the work placements are optional and it is up to the students to arrange them. Recently some public universities allow students to gain credits through summer internships, and this initiative has a high interest for students, who are eager to gain work experience, even without getting paid, because the vast majority of job openings require work experience.
- **The cost of professional certifications.** One of the top priorities of many ICT professionals is the acquisition of professional certifications; both vendor specific (Microsoft, CISCO, ORACLE, HP) and independent bodies (ISACA, ECDL). As these certifications frequently appear within ICT related vacancy announcements, their possession increases employment opportunities and enhances career development prospects. The acquisition of ICT professional certifications is not subsidized by the HRDA (Human Resources Development Authority – see www.hrdauth.org.cy). And most of the up-skilling and other training programs subsidized by the HRDA are not accredited with a certification process upon completion. The high cost of these certifications is a barrier for many ICT professionals to pursue them. ICT companies must invest in developing soft skills by recognizing the importance of project management and other non-technical skills such as presentation and time management for ICT professionals.

To reinforce the IT security skills in Cyprus, several lines of actions are open. Among them, priority will be to support the securing of experience by graduates, by facilitating work placement (develop a formalised work experience programme and degree programmes which combine theoretical education at the University, and practical experience with an ICT company; set-up a web portal to advertise students; encourage and offer incentives for SMEs to offer traineeships…) and promote the use of real-world project in the Universities' courses. Another priority is work on the employment paradox, by supporting the recruitment of local qualified persons instead of looking to attract skilled talent from other countries (support the up-skilling of employed and unemployed ICT professionals by defining a minimum and mandatory amount of training or credits every year for ICT professionals).

5 Conclusion

In conclusion, Europe and BeWISER regions face a number of common challenges. The three main challenges that need to be addressed to meet the ongoing IT security skills shortage are described below:

1. **The training challenge**
    - **Initial training:** the need of developing **new and adapted courses** in collaboration with Universities and Schools. Particular attention will be paid on the **on-going adaptation of curricula** to be aligned with industry expectations and to follow the rapid changes in ICT and IT security; and on the opportunity **to gain practical experience, via apprenticeship type arrangements,** during the training programme in partnership with ICT companies and especially SMEs. This implies **reinforcing the proximity between HEI and ICT industry**.
    - **Life-long learning:** the need for investment by companies, especially SMEs to develop the **new and necessary competencies** of their employees through **on-going training** for the IT staff. Particular attention will be paid on the removal of barriers (financial, administrative, organisational, etc.) for SMEs to put in place such training.

2. **The attractiveness challenge**
    - **Students:** the need of making ICT security attractive for students, by **demonstrating the jobs and opportunities** of the security field.
    - **Employees**: the need to reverse the brain drain, whilst also encouraging mobility and being attractive for new graduates or persons with competences and experiences, by **offering them a good working environment / conditions.**

3. **The awareness challenge**
    - The need for security **awareness training for all the stakeholders of organisations**, and not only the core IT workers : employees, managers and corporate boards

The triple helix clusters of the BeWiser project are well placed to help shape, support and design suitable solutions to these challenges. For example they can:

- Inform HEI's of the needs of the business community;
- Source and facilitate entrepreneurships and help match needs, especially for SMEs
- Support efforts to put in place and promote Cyber security related accreditation initiatives
- Enhance awareness raising issues by working with national cyber security agencies

6 Bibliography

6.1 Article

THOMAS WADLOW, "*Top 10 IT Skills in Demand for 2015"* - 2015
Available Online: http://www.businessrevieweurope.eu/technology/380/Top-10-IT-Skills-in-Demand-for-2015

UPASANA GUPTA (CareersInfoSecurit), *"5 Most In-Demand Security Skills"* - 2012
Available Online: http://www.bankinfosecurity.com/5-most-in-demand-security-skills-a-4934/op-1

STUART REED (NTT Com Security), "*The IT skills conundrum: too many threats and not enough professionals"*- 2014
Available Online: http://www.information-age.com/technology/security/123458368/it-skills-conundrum-too-many-threats-and-not-enough-professionals

TOBIAS HÜSING, WERNER B. KORTE, ERIONA DASHJA (empirica) - "*E-skills and e- leadership skills 2020 - Trends and forecasts for the European ICT professional and digital leadership labour market"* - Working Paper 2015
Available Online: http://eskills-lead.eu/fileadmin/LEAD/Working_Paper_-_Supply_demand_forecast_2015_a.pdf

WISER (European Innovation Action project) - "*Cyber Security Skills Shortage should not be underestimated"*- 2015
Available Online: http://www.cyberwiser.eu/news/cyber-security-skills-shortage-should-not-be-underestimated

6.2 Report

WORLD ECONOMIC FORUM - "*Global Risk 2014: Ninth Edition"* - Insight Report 2014
Available Online: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

FROST & SULLIVAN, "*Critical Times Demand Critical Skills - An analysis of the skills gap in information security"* – A whitepaper derived from the (ISC) Global Information Security Workforce Study
Available Online: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/GISWS-Skills-Gap-Analysis.pdf

PROGRESS CONSULTING S.R.L. & THE NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS "*European Internet Security Strategy*"- Report April 2013
Available online: http://cor.europa.eu

NICOLAI SØNDERGAARD LAUGESEN & ALL. (Fraunhofer & Danish Technological Institue) - "*Cloud Computing, Cyber security and Green IT – The impact on e-skills requirements"* – Report prepared for the European Commission – April 2012
Final brochure available online: http://ec.europa.eu/DocsRoom/documents/10474

KARSTEN GAREIS, TOBIAS HÜSING, STRAHIL BIROV, INNA BLUDOVA, CAROLA SCHULZ, WERNER B. KORTE (empirica) - "*E-skills for jobs in Europe: measuring progress and moving ahead"* – Report prepared for the European Commission – February 2014
Available Online: http://eskills-monitor2013.eu/results

6.3 BeWISER inputs

ISABELLE DE SUTTER, PIERRE DIDIERJEAN, LEA LANAUD (Systematic) - "*Ile-de-France - Consultative Policy Roundtable*" – May 2014

DAVID MARÍ (Bdigital) - "*Catalonia - Consultative Policy Roundtable*" – June 2014

TAMARA HÖGLER, RALF TRUNKO AND MARTIN HOFMANN (Cyberforum) - "*TechnologyRegion Karlsruhe - Consultative Policy Roundtable*" – May 2014

DR JOHN HOBBS, EOIN BYRNE, MICHAEL WALSH, DARRAGH O'SUILLEABHAIN, EILEEN CROWLEY, ELAINE WALSH (Cork Institute of Technology, South West Regional Authority, IT@Cork) - "*South West Region - Consultative Policy Roundtable*" – May 2014

PHILLIP MILLS (QUB – CSIT), MICHAEL NOBLE (Momentum NI), ROBERT BUNN (Invest NI) - "*Northern Ireland Region of the United Kingdom - Consultative Policy Roundtable*" – June 2014

NINA SEGA, TOMAŽ VIDONJA (ICT Technology Network) - "*Slovenia - Consultative Policy Roundtable*" – May 2014

PANICOS MASOURAS, IOANNA DIONYSIOU, HARALD GJERMUNDROD AND GEORGE BEITIS (CCS) - "*Cyprus - Consultative Policy Roundtable*" – May 2014

ALEX JOYCE, EOIN MOYNIHAN BRIAN CAHILL (Cork Institute of Technology) - *"Market Analysis"* – Deliverable 2.3 Report - April 2014

SORAYA BERNARD, MARIANNE BAUMBERGER, ADÈLE SCHWARTZENTRUBER, LUC SCHMERBER, MARC PATTINSON (inno) - "*Partner-wide SWOT analysis and Joint Working Plan"* - Deliverable 2.4 Report - June 2014