D5.3.1 – Executive Summary of D5.3 "Report of best practice in sectors other than Security"

Due date of deliverable: 31/01/2013

Actual Submission date :03/03/2013

Deliverable ID: D5.3.1
Deliverable Title: Executive Summary of D5.3 **"**Report of best practice in sectors other than Security"
Responsible beneficiary: Michael Remes (EFPC (UK) Ltd)

Dissemination level: Public
V1.1 (updated 29th May 2013)

Start Date of the Project: 01/04/2012 (24 Months)

Table of Contents

Introduction

This report is a summary of D5.3 describing best practice in sectors other than Security. Please refer to the full report for more detailed information.

0.1 Interviews

In addition to the End-User interviews in the Security domain described in D3.3 (Assessment results analytic report), INSEC Consulting Partners (ALMA, EFPC, FMMC, ADVISIO, EVERIS, INOGATE) and some end-user partners (ORFK, PAG, BIA, EASS) conducted interviews targeting sectors other than the Security. This included: General Consultancy, Environment, Telecommunications, Transport, Aerospace and Defence, Higher Education, Health, ICT, Transport. The purpose of these interviews was to identify innovation practices in non-security sectors.

Interviews were carried out until 31 January 2013 with organisations in industries other than the Security domain. 16 interviews were conducted. Of the organisations interviewed, 10 are SMEs and 9 are from Eastern European and Baltic Countries. Interviews were conducted with organisations in Estonia, France, Hungary, Romania and Spain. The majority of the organisations interviewed are from the private sector.

0.1.1 Themes within the Interview Script

The interview questionnaire design follows the conceptual and methodological architecture defined for characterising the four segments involved in the project. It is based on two accepted models: (1) COTIM (providing an «internal» perspective) and (2) The Triple Helix (providing an «external» one). These models are described in detail in INSEC D3.2 "Segment innovation ecosystem report".

The questionnaire was broken down into the following sections:

- Corporate Culture (Innovation Policy, Innovation Culture)
- Corporate Strategy (Formulation of the innovation strategy, Deployment of the innovation strategy)
- Management (managing implementation of the innovation strategy)
- Organisation (Training for innovation, Organisational structure supporting innovation, Innovation Skills, Motivation)
- Knowledge (Mechanisms for identifying external knowledge sources)
- Processes (In this report, Processes focuses on the procedures in place to guarantee observance of legal, regulatory and ethical issues e.g. data protection)
- Technology and Tools (Infrastructure for innovation, Technology, Tools)
- Collaboration and Networking (Relationship Model, Innovation Financing)

The results from the questionnaires summarised below give both formal and informal awareness of innovation inside the organisations that have been interviewed. The most mature and innovative organisations are coming from more developed countries in Western Europe.

0.2 Best Practice collected via Desk-Research in industries other than the Security domain

Additional research into Best Practices in the themes described in section 1.1.1 of D5.3 was carried out in order to supplement the findings of the interviews and go into more depth regarding points raised from the interviews and the subject matter in general.
Research included recent studies, surveys, on-line articles, relevant books etc. on subjects including Innovation Management; Open Innovation; Innovation Networks; Structured Crowdsourcing; Incentive Prize Competitions; Studies and Surveys; Knowledge Maps. Researched sectors include Health, Retail, Telecoms, Games, ICT, Transportation, Security, Film industry.

Section 1: Corporate Culture

Ensure innovation is part of the organisation DNA

The elements that make up a truly innovative company are many: a focused innovation strategy, a winning overall business strategy, deep customer insight, great talent, and the right set of capabilities to achieve successful execution. More important than any of the individual elements, however, is the role played by corporate culture — the organisation's self-sustaining patterns of behaving, feeling, thinking, and believing — in tying them all together.

Companies that are leading innovators such as Merck, P&G and DOW-Chemicals not only have innovative leaders, but more importantly they have leaders who create conditions that facilitate innovation by encouraging, measuring and incentivising collaboration.

Include innovation in vision and mission statements

These actions will enable formulation of the "non-spoken" and create awareness about the fact that the organisation is innovative.

Build an innovation strategy

Use performance indicators aimed at defining needed resources and expected outcomes for activities.

Enhance internal innovation with specific communication tools and processes

Web-based idea collection software, focus groups, brainstorming, creativity workshops should all be norms, habits and practices within the security end-user organisation. This also applies to the constant re-defining and monitoring of performance indicators, expected outcomes and needed resources.

Create an innovation culture on organisational level

The leading innovative companies invest in creating an environment that allows innovation to thrive while encouraging employees to feel comfortable taking calculated risks.

Periodically disseminate organisational values to employees

The tighter the connections between strategy, culture, and innovation, the more effective the organisation will be converting innovation spending into marketplace results and efficient use of financial resources. As part of these activities, the articulation and dissemination of an organisation's values to its employees is important and should be periodically updated.

Use company culture as an innovation accelerator

The inclusion of a top-to-bottom and bottom-to-top communication flow, by creating formal processes (regular executive meetings between technicians and top management) and a detailed action plan are necessary to put innovation into action.

Focus on people and push them beyond existing boundaries

Employees will be reluctant to take risks inherent in Innovation unless they know that their leadership team is willing to accept a certain amount of failure as an inevitable part of the Innovation process.

Learn more about brainstorming methods

As corroborated by the survey feedback, Brainstorming is an important Best Practice. There are many techniques for Brainstorming and good examples can be found in Bryan W. Mattimore's book "Idea Stormers: How to Lead and Inspire Creative Breakthroughs.

Section 2: Corporate Strategy

Adopt innovation when defining/changing company strategy

The role of strategic planning as a key element in the management system is explicitly recognised through strong links to other elements of the management system (e.g. strong human resources and organisational structures).

No strategy is effective forever. Something in the external environment eventually changes--new technology appears, customer needs shift, new competitors emerge--rendering it ineffective. The temporary nature of successful strategy means that organisations should continually scan the external environment for threats and new opportunities. Strategy formulation is an on-going requirement of good management, and a process that should be permanently embedded in the Security end-user organisation.

Leading organisations continuously monitor and review strategy. Outside views can be powerful. Some firms, particularly those in technological fields, enlist teams of scientists and engineers to look outward to markets, competitors, and technical developments. Resources and internal capabilities can constrain an organisation's choice of strategy. A strategy to exploit an un-served market might not be feasible if the organisation lacks the necessary financial capital and human know-how.

Define innovation plan objectives consistent with the outlined innovation strategy

A strategy can succeed only if it has the backing of the right set of people and other resources. Alignment between the people and the activities of the organisation and its strategy is critical to the implementation of strategy. Strategic planning requires participation and periodic input from all levels of the organisation. Alignment is a condition in which every employee at every level understands the strategy, and understands his or her role in making the strategy work.

Identify operational elements of an Innovation Action Plan

The innovation strategy must be aligned with an implementation action plan which is communicated, understood and actualised by all employees in the organisation through their day-to-day activities. An innovation action plan must contain elements that will allow it to be continually monitored and reviewed including: objectives, targets/indicators, indicative resource allocation, timeframes and budgeting. It is also essential that the implementation plan, in today's global digital world includes activities to counter cyber-attacks and strengthen security in government organisations.

Section 3 and 4: Management and Organisation

Use action plans and continual assessment

Organisations should review their performance and plan for the future on an on-going basis. Knowledge of the competition is important to understand and benefit from their best practices, and learn from their mistakes. Also important is continual review of employee capabilities within the interviewed organisations for determining customer requirements and delivering results.

The organisation's performance should be continually reviewed against performance indicators and effectiveness of allocated budgets at board level, departmental level and project level. To support these performance levels, innovation management and procedures should be incorporated in the quality control

procedures of an organisation which should also include security procedures to protect organisation assets including data and IT infrastructure.

Manage innovation using quality control standards

Implementing work using quality control standards can help e.g. ISO 9001.

Focus on Employee Skills

Employees are the number one asset and it is therefore of the utmost importance that people with innovation potential and commitment are identified at the recruitment stage. Also important is that employee profiles and skill-sets match the needs of the companies and skill-gaps are identifiable and continually monitored. Continual training and seconding of staff between departments are important facilitators.

Create an innovation focused organisation structure

An organisation's structure should be readily able to deal with unforeseen actions and chance occurrences, which are characteristic of innovative environments. End-User security organisations should consider more flexible and agile organisational structures that allow interaction and communication between employees, without rigidly defining functional areas within the organisation.

In more turbulent, complex, and uncertain environments, such as innovative ones, static organisational frameworks with rigid division and specialisation of labour cannot provide the flexibility and agility needed to maintain innovative competitiveness. Organisation and communication structures that encourage and make use of experience-based learning, knowledge sharing, and interaction – such as project teams, problem solving groups, and task rotation – can contribute positively to the performance of innovative activities"

Motivate your staff

Many leading organisations encourage staff to be innovative through specific schemes, but appreciation by management and peers is the best motivation. To maintain the enthusiasm employees bring to their jobs, management must understand three sets of goals that the great majority of workers seek from their work—and then satisfy those goals:

- Equity: To be respected and to be treated fairly in areas such as pay, benefits, and job security.
- Achievement: To be proud of one's job, accomplishments, and employer.
- Camaraderie: To have good, productive relationships with fellow employees.

Robin Speculand notes in his book "Beyond Strategy" that in a study of 1,500 employees conducted by Dr Gerald Graham, a professor of management at Wichita State University, personal congratulations – by managers of employees who do a good job – was ranked first from 67 potential incentives he evaluated!

Empower your staff

People have to empower themselves. It is not possible for a leader to "empower" someone to be accountable and make good decisions. The leader's role is to encourage and support the decision-making environment, and to give employees the tools and knowledge they need to make and act upon their own decisions. By doing this, leaders help their employees reach an empowered state.
Employees understand their jobs, and know their tasks, roles, and functions within the organisation. Organisation leaders should therefore let them do what they need to do to get the job done.

Ensure IT security

In today's society, organisations are dependent on IT to a very large extent. As a priority, these organisations must protect their assets against criminal and terrorist activities. Especially vulnerable are large industrial organisations and end-user security organisations. There are plenty of high-profile breaches of security which have resulted in large financial costs and infringement or loss of confidential/private data.

Section 5: Knowledge

Organisations must continually source new knowledge

In order to be innovative, organisations must identify new opportunities in their market place and the techniques and methodologies necessary to produce new products and services. This includes products and services required internally by organisations to create greater efficiencies and more effective processes or/and required externally to sell to existing and potential customers in order to remain competitive.

Security organisations must continually monitor their ecosystems for new and emerging knowledge, technologies and trends through contact networks, business partners, Universities, research institutes and attending conferences, seminars and other sectorial events. Organisations should also receive regular feedback from customers and through networks of experts. Other sources of information include sector-specific journals/magazines, databases etc.

Public-private partnerships can be used to jointly fund projects

Gaining and implementing new knowledge requires continual development of current and new partnership and cooperation agreements with relevant SMEs and other organisations in the organisation ecosystem.

Use Open Innovation

In today's global digital society, where the potential to access people and organisations has never been easier, Open Innovation is an important tool for capturing external knowledge. Incentives, prizes, competitions, Open-platforms, Open-source, Innovation Networks, Crowdsourcing are all examples of methods of engaging with external parties that can have an impact on an organisation in terms of improving and developing products and services as well as solving technical or other issues.

Organisations must manage and share knowledge inside their organisations

From a knowledge-management perspective, large organisations require internal systems to capture knowledge, protect and share it; especially in big companies it is very easy to "re-invent the wheel" resulting in inefficient use of resources. Tools such as: Intranet, Blogs, customised software, databases and Wikis can all be used in an integrated manner.

Section 6: Processes

Create methodologies for systematising innovation

Use methodologies to help structure innovation processes. Examples include: Total Quality Management, Six Sigma and Benchmarking.

Address legal, regulatory and ethical issues

Organisations must comply with relevant national, European and international regulations, standards and laws pertinent to their sectors and continually monitor them for any updates on an on-going basis. For example: Ethical Committees, Regulatory Bodies (legal issues), procurement rules, standards, legal requirements. Organisations should employ software and tools to assist in the storage of information and compliance with these rules and regulations, including the ability to flag to necessary personnel in case of any breaches or oversights

Ensure protection of confidential data

Privacy and data protection should be considered and embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal.

Work in an ethical way

Ethical issues can pertain to Informed Consent, Privacy, Research on animals, research involving development countries, dual use (Research having potential military/terrorist application). It is important organisations have policies and procedures for dealing with these issues e.g. ethical committees, and complying with national, European and international rules and regulations.

Section 7: Technology and Tools

Continually monitor and review new technologies and technology trends

To remain competitive organisations need to continually monitor emerging technologies and technological trends and identify partners and providers, who they can collaborate with to produce innovative solutions to identified issues.

- **Technology Watch** - Technology Watch is essential for identifying tools and resources to assist Security End-User organisations, not only to become more efficient and futuristic, but also from a security viewpoint to continually keep at least one step ahead of terrorist and criminal threats. E.g. Cyber-terrorism is a great concern. These tools therefore also need to monitor activities on social networks such as Facebook and Twitter, in order to identify potential threats.

- **Technology Platforms** - In Europe, the Technology Platforms (http://cordis.europa.eu/technology-platforms) established in different industry sectors, are good points of reference for researching new technologies and trends, as well as networking with key stakeholders.

- **Cross-Border Collaboration** - Active cross-border collaboration between end-user security organisations. Cross-border communication is essential between Security end-users in different countries not only to identify new technologies, but also to collaborate in the joint implementation of these technologies by forming partnerships against crime.

Identify technology providers

Information overload is upon us and it is therefore important to be able to access the right information and people who can assist organisations become more innovative. Using the correct networking and collaborating tools will assist organisations reach the right people and achieve the results they are looking for.

D&A Knowledge Maps are a good example of best practice for creating knowledge maps identifying and profiling organisations and players in an end-user organisation's eco-system, including potential SME and industry technology providers. An example is the Israel Homeland Security Sector. Other examples can also be found at http://search.dainfo.com/hls_israel/Template1/Pages/StartSearchPage.aspx

Section 8: Collaboration and Networking

Identify customer and stakeholder needs and requirements

Customer and stakeholder needs can be identified via: attending events and conferences; access to experts' networks; collaboration with RDI centres, technological parks, industrial platforms, research departments; access to and active involvement with networks (e.g. Enterprise Europe Network) and EU Technology Platforms; Framework Program projects etc.

- Use a dedicated website where clients can give input, or a method for determining customer satisfaction.
- Consulting companies can assist organisations determine products or services they could offer customers.
- Conduct feasibility studies and market research before implementing an innovation project.
- Form partnerships with other end-user security organisations for the purpose of joint R&D projects, either in the same country or cross-border.

Protect Intellectual Property (IP)

The protection of intellectual property rights is essential and a key aspect when working with external parties. IP can be protected via patents and confidentiality agreements. External advisors can assist e.g. patent lawyers. The European IPR Helpdesk (www.iprhelpdesk.eu) offers free of charge, first-line support on IP and IPR matters to beneficiaries of EU funded research projects and EU SMEs involved in transnational partnership agreements.

Focus on fund-raising activities

A good practice is to have a department or sub-department dedicated to fund-raising activities. FP7 and Horizon2020 funding and other national, European and international public funding can be used as a major source of monies for R&D and infrastructure. Other funding sources that may be considered are external private funds, venture capital and public-private partnerships.

- Large organisations can perhaps invest money from internal funds made available by their organisations.
- Public organisations such as end-user security organisations may consider jointly financing an R&D initiative with private organisations including SMEs.

D5.3 Conclusion

From the research carried out in producing D5.3 it is clear that Strategy determines the required culture in an organisation and not the other way round. Importantly, the culture of the organisation is important for driving the implementation of the strategy. Conversely, this means that organisation leaders must identify an implementation approach that fits the culture.

"If the implementation of the strategy moves too fast for the culture, you end-up overpromising and under-delivering – and the effort crumbles."[1]

It should also be noted that the public sector in Europe and especially in poorer regions faces budget reduction and increased requests for services (qualitative and quantitative); processes and methods related specifically to Innovation are therefore less of a priority. Interview results show that organisations from Eastern European and Baltic countries, in general terms do not have specific processes in place to manage innovation. Only recently has the EC declared INNOVATION as a flagship initiative at European level in order to solve this issue.[2]

The majority of Eastern Europeans and Baltic Countries are followers (a notable exception is Estonia which, according to the EU Innovation Scoreboard for 2011, show a performance close to that of the EU27 average) and will copy and adapt best practices developed in western and other more developed countries in order to reach higher levels of innovation. For example, Romania does not have a dedicated Policy for Innovation: innovation was included within the national Research and Development Strategy 2007-2013 but without having defined clear targets, plans, objectives, resources. The importance of best practices and their dissemination is therefore especially relevant for Eastern European and Baltic countries.

To summarise, the following are important examples of Best Practices that should be considered by Security end-users as part of their innovation strategy:

At most innovative organisations, job definitions tend to be flexible and fluid. These companies recognise that the roles their employees play must adapt to the changing needs of the marketplace. As a source at Dow Chemicals put it, "It's empowerment that really helps us stay agile. We encourage everyone to lead courageously — constantly asking "what if?" or "why not?" We challenge our employees to recognize possibilities and push beyond boundaries."

A strategy can succeed only if it has the backing of the right set of people and other resources. Strategic planning requires participation and periodic input from all levels of the organisation. No strategy is effective forever. Something in the external environment eventually changes--new technology appears, customer needs shift, new competitors emerge--rendering it ineffective. The temporary nature of successful strategy means that organisations should continually scan the external environment for threats and new opportunities. Strategy formulation, then, is an on-going requirement of good management, and a process that should be permanently embedded in the Security end-user organisation. There is no single "best practice" for how to do successful strategic planning. The timing and process will differ depending on the security sector, market pressures, and the size and culture of the organisation.

End-User Security organisations should consider more flexible and agile organisational structures that allow interaction and communication between employees, without rigidly defined functional areas, and with functional integration instead. This would permit the development of knowledge based on practical experience and interaction, consequently leveraging the organisation's innovative capacity[3]. This

[1] Quotation from "Beyond Strategy", a book written by corporate strategy expert, Robin Speculand
[2] http://ec.europa.eu/research/innovation-union/index_en.cfm
[3] Jensen et al., 2007

organisational configuration would also be more readily able to deal with unforeseen actions and chance occurrences, which are characteristic of innovative environments.

- There are many examples of Open Innovation which organisations can use to reach out to potential customers, suppliers and collaborators. These include: joint R&D collaboration with Universities; competitions enticing customers and users to come up with new ideas; crowdsourcing to solve problems amongst wide groups of experts physically located in different locations worldwide; enabling customers to beta-test and give feedback to new products and services.

- It is good practice for an organisation to have experts employed in areas such as IPR, legal and ethical, but if not the case outside experts or specialised consultancy organisations can be used. It is important that organisations are reviewing on a continual basis updates to standards, regulations and laws etc. on an on-going basis to ensure their compliance.

- In Europe, the EU Technology Platforms (http://cordis.europa.eu/technology-platforms) established in different industry sectors, and also EU Framework Program projects operating in the area of Technology Watch are good points of reference for researching new technologies and trends, as well as networking with key stakeholders. Also important is attending European conferences related to the Security sector. Cross-border communication is also essential between Security end-users in different countries not only to identify new technologies, but also to collaborate in the joint implementation of these technologies by forming partnerships against crime.

- A major problem for Security end-users is that European research is very fragmented and therefore it is difficult to find the "right" organisation or new technology as they are not visible. To solve this problem, clustering of organisations in different security sectors is an important activity and currently facilitated by EU Framework Program projects such as SIGNATURE, and organisations such as Enterprise Europe Network (EEN). In addition mapping of different sectors' ecosystems needs to be implemented, including profiles of organisation involved in the chain.

- Once collaboration opportunities have been identified, funding becomes an important issue. There are many local, National and European funding instruments that can assist (e.g. FP7 and Horizon2020), in addition to various venture capital funds. Also, public organisations such as end-user security organisations may consider jointly financing an R&D initiative with private organisations including SMEs.

INCREASE INNOVATION AND RESEARCH WITHIN SECURITY ORGANISATIONS

COORDINATOR
ALMA CONSULTING GROUP SAS
(+33 (0) 4 72 35 80 30)

PARTNERS
EFPC (UK) LTD
FM MANAGEMENT CONSULTANCY SRL
PROXIMA CENTAURI SAS
ADVISIO OU
GLOBAZ SA
EVERIS SPAIN SLU
INOGATE- CONSULTORIA EM INOVACAO EMPRESARIAL SA
SISEKAITSEAKADEEMIA
ACADEMIA DE POLITIE ALEXANDRU IOAN CUZA
GRAD SKOPJE
AUTORIDAD PORTUARIA DE GIJON
HUNGARIAN MINISTRY OF INTERIOR
OU BALTIC INNOVATION AGENCY B.I.A.
ROMANIAN MINISTRY OF ADMINISTRATION AND INTERIOR
GNS - GABINETE NACIONAL DE SEGURANÇA

SEVENTH FRAMEWORK PROGRAMME

INSEC is a project co-funded by the European Commission under the Seventh Framework Programme (2007-2013).