IPACSO: Towards Developing an Innovation Framework for ICT Innovators in the Privacy and CyberSecurity Markets

Zeta Dooly[1], Seamus Galvin[2], Jamie Power[3]*, Bart Renard[4] and Ulrich Seldeslachts[5]

TSSG, Waterford Institute of Technology, Waterford, Ireland, [2] Espion Ltd., Dublin, Ireland, [3]RIKON, Waterford Institute of Technology, Waterford, Ireland, [4]Vasco Data Security, Wemmel, Belgium, [5]LSEC, Leuven, Belgium

{Zeta, Seamus, Jamie, Bart, Ulrich}@ipacso.eu

A pressing challenge facing the cybersecurity and privacy research community is transitioning technical R&D into commercial and marketplace ready products and services. Responding to the need to develop a better understanding of how Privacy and CyberSecurity (PACS) market needs and overall technology innovation best-practice can be harmonized more effectively the contribution of this paper is centred upon the development of a set of innovation guiding principles to inform the overarching IPACSO (Innovation Framework for Privacy and CyberSecurity Opportunities) innovation framework to be developed. These guiding principles have been developed from ongoing market and economic analyses and innovation modelling research in an effort to explore the identification of PACS specific deltas with respect to innovation. The development of the innovation guiding principles represent a pivotal component in meeting IPACSO's overall goals of supporting increased awareness of and engagement in innovation practices, in addition to supporting greater knowledge of market dynamics, barriers and solution potential for increased innovation activity in the domain.

Keywords: innovation, framework, guiding principles, privacy, cybersecurity

1 Introduction

The publication of the EU CyberSecurity Strategy [1] and the progress in relation to the proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union has and continues to impact the privacy and cybersecurity market. With clear objectives to encourage economic growth as people's confidence in buying things online and using the Internet is

strengthened, opportunities for innovators in this domain is increasing. Nonetheless, a range of challenges including, but not limited to: pursuing a narrow innovation process failing to incorporate the internal and external ecosystem or customer needs, an overemphasis on technology-driven bottom-up innovation, in addition to unsupportive deployment channels for research output/commercialization's hamper the transitioning of technology related research developments and outputs to commercial deployment [2]. Compounding the above challenges, the privacy and cybersecurity (PACS) domain is deeply influenced from various themes driven by technical, human, societal, organizational, economic, legal, and regulatory concerns among others; these factors combine to create marketplace and innovation ecosystem with complex value chain relationships [3]. Mindful of this, this paper outlines IPACSO's methodological approach to develop a series of innovation guiding principles to inform a knowledge and decision-support framework for identifying, assessing and exploiting innovation opportunities across the PACS domain.

While a significant general body of information around innovation exists i.e. the set of rules, models and stages involved [4]; the contribution of this paper is centred upon the development of a set of innovation guiding principles to anchor the overarching innovation framework to be developed. These guiding principles are informed from ongoing market and economic analyses and innovation modelling research to explore the identification of PACS specific deltas with respect to innovation. Through a specific PACS lens, IPACSO therefore aims to support innovators in both industry and research communities with a responsive innovation framework to enhance their overall innovation engagement, management and deployment activities. Additionally, IAPCSO aims to support and provide relevance to academic, policy making and related innovation enabling and funding stakeholders in terms of providing guidance and support to innovation activities. In this vein, IPACSO seeks to refine generic innovation guidance to the PACS domain and stakeholder needs to support innovators via decision support guidance and toolkits to identify the potential and scope of opportunities in addition to highlighting innovation tactics specifically for this market.

Regarding the structure of this paper; firstly the rationale for an innovation framework is presented, followed by an overview of the IPACSO methodological approach, and culminates in the identification of the initial guiding principles which will anchor and inform the development of the IPACSO Framework.

2 Rationale for an Innovation Framework

A pressing challenge facing the cybersecurity and privacy research community is transitioning technical R&D into commercial and marketplace ready products and services – "New and innovative technologies will only make a difference if they are deployed and used. It does not matter how visionary a technology is unless it meets the needs and requirements of customers/users and it is available as a product via channels that are acceptable to the customers/users" [2]. While innovation is widely recognized by industry and academics as a sustainable and competitive enabler, none-

theless understanding of innovation management and practice remains fragmented, misunderstood and untamed by practitioners and researchers [4].

Innovators operate within complex and turbulent environments, and are increasingly confronted with escalating and rapid technology developments, competitive global market competition and shorter product life cycles meaning they must be reactive and flexible to organizational, technological and market shifts [5]. Indeed, the privacy and cybersecurity market is deeply influenced from various themes driven by technical, human, societal, organizational, economic, legal, and regulatory concerns among others; these factors combine to create marketplace and innovation ecosystem with complex value chain relationships [3]. Innovation therefore, cannot not occur within a vacuum and is impacted upon by a range of external contextual factors in addition to the following internal considerations, including but not limited to, strategy and culture, resources and skills, leadership, organizational structure and external linkages [6], [7], [8].

Reflective of the above, innovation practice is far from straightforward "…most innovation is messy, involving false starts, recycling between stages, dead ends and jumps out of sequence" [4]. Indeed, it is argued that the problem does not lie in the generation of innovative ideas, but more in the successful management of the innovation process from an idea to a successful product in the market [9]. As cited by [10], Booz Allen Hamilton found that a common denominator in terms of transitioning new products to market is the utilization of a defined process for managing innovation incorporating stage approval and measurement processes across critical components. In a similar vein, the 2013 iteration of The Global Innovation 1000 Survey [11] identified that the level of R&D investment is not exclusively what determines innovation success; as how R&D funds and efforts are invested in capabilities, talent, processes and tools significantly impacts upon innovation development efficiencies and success.

3 Methodology

In pursuit of the development of a knowledge and decision-support innovation framework in the privacy and cybersecurity technology space, the IPACSO project is guided by an overarching three-staged methodological approach, as synopsized below.

IPACSO is an EU-funded Coordination and Support Action (CSA) project aimed at supporting Privacy and CyberSecurity innovations in Europe. IPACSO is focused on adapting existing innovation methodologies available in other domains, both general and specific; optimizing these approaches for the Privacy and CyberSecurity (PACS) market domains. Ultimately, IPACSO will combine innovation support modules based on established Methods (both generic and technology-specific), with new innovation support approaches geared towards the specific needs of the European PACs marketplace.

Stage 1: Development of a PACS innovation knowledgebase that will provide a detailed, yet intuitive understanding of the cybersecurity and privacy innovation space industry, market and value chain assessments, product and industry taxonomies, PACS (economic insights and considerations, innovation model overviews).

Stage 2: Development an analytical and decision-support framework for innovation management, macro analysis and product and ideation to enable innovators to identify, assess, prioritize and execute product ideas in a rigorous, market-centric manner.

Stage 3: Proof of concept and validation of the developed framework on several levels, via iterative stakeholder engagement. IPACSO framework content will also be validated iteratively, via bootcamp events and through related dissemination and exploitation events and programmes.

For the purpose of this paper, Stage 1 takes centre stage and the methodological direction involves the triangulation of emerging findings from three parallel work-in-progress research streams to inform the identification of a series of guiding principles to anchor the overarching IPACSO innovation framework to be developed.

3.1 PACS Market Analysis

The PACS marketplace has experienced significant growth in recent years, with further overall growth anticipated on both EU and global levels between now and 2020. Globally the market is presently valued at €62.4bn per annum, with a 13.4% global annual growth predicted between now and 2020, leaving an anticipated 2020 market of over €111m [12]. The EU market is presently worth approximately one-quarter of the global market at €16.5bn, with just under 10% growth per annum predicted within the region, leaving a future potential EU market of €25.1bn by 2020.

Existing and future growth in the PACS space is driven by a number of key trends, including an ever increasing number of threat vectors in which ICT infrastructure can be compromised, driven by more diverse and pervasive emerging technologies (e.g. mobile, Internet of Things and cloud infrastructures), increasing regulatory initiatives making security and data breach notifications mandatory (e.g. EU Data Protection Directive [13], NIS Directive [14], increased technology standardization leading to security exploit information being readily available to attackers, and via increased security spending both internally and via outsourcing. Many commercial organizations are also moving away from viewing security as just a "tick the box" initiative, increasingly purchasing security in response to genuine fears of data breaches and other security threats. Exponential data growth is also another security market driver as privacy risks increase in line with growing data volumes and ease at which datasets can be de-anonymized. Data growth is also a driver of security technology innovation, as effective security monitoring and mitigation increasingly becomes a "big data" problem.

Within the PACS domain several challenges exist around bringing new innovations effectively to market. Key solutions in the domain are of a technically complex nature, generally developed by highly technical individuals with significant experience in the industry, many staying in the industry for long periods as serial entrepreneurs [15]. In addition, while the military and government space demands one-off bespoke solutions, the marketplace for PACS solutions serving general commercial requirements is highly saturated, with an ever growing array of PACS technology options. This is reflected in the year-on-year growth in attendees at key industry conferences such as RSA (this year's conference had 340 vendors exhibiting in the data security category alone) [16]. Such product saturation makes it difficult for PACS innovators to differentiate products from other offerings, to accurately evaluate their own product features versus those of competitors due to the vast competitive knowledge necessary, and ultimately for customers to find time to understand differences between products, especially when product benefits sound similar at the marketing level. This often leads to poor product decision making, and the cheapest alternative being purchased as opposed to the most effective one.

Other challenges relate to the reality that security is purchased as a risk mitigation measure rather than providing any direct return on investment value itself – making value justification arguments more difficult for PACS vendors to make, when the solution's value is related to some future security event whose timeline is unknown in advance [17]. Effective security ultimately involves people, process and technology elements, so consultancy and service expertise is also necessary to sell security products effectively. This is reflected in some of the high-profile M&A activity in the space where key product vendors (e.g. FireEye) are acquiring outside service and consultancy expertise (ala Mandiant) [18]. Challenges of moving PACS innovations from prototype to adoption and integration in real world environments can also pose barriers and challenges.

Aside from strong internal capabilities in technology product management and innovation models and processes, PACS innovators with appropriate access to the best innovation ecosystems and environments are also at a key advantage. Key ingredients supporting such optimal environments include sustained access to the hardest cyber security and privacy problems (i.e. within military and large organization settings), a strong cyber-academic base, access to a sustained skill and talent flow of scientists and engineers, appropriate funding and mentoring supports from venture capitalists and similar commercial investors, backed up by strong government leverage around commercially backed investments. Flexible tech-transfer terms and appropriate logistics and ease of human interaction within the innovation hub are also ideal ingredients [19].

3.2 Innovation Models

Innovation models are important because they assist management teams in framing, understanding, and acting on the issues which need managing [20]. For this reason a review of innovation models is presented to illustrate the interrelated stakehold-

ers, processes and issues which need to be factored into an overarching innovation framework.

It is cautioned that if innovation models are limited the subsequent innovation management and delivery approach will also be hampered [4]. Understanding of the process of innovation at the firm-level has evolved throughout recent decades from simplistic 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 [6] documented five shifts or generations, as synopsized below [4], [6], [10], [20], [21], demonstrating that the complexity and integration of the models increases with each subsequent generation as new practices emerge to adapt to changing contexts and address the limitations of earlier generations [21].

The *first generation technology push era* of innovation models represents a simple linear structure which mapped 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. In the *second generation market pull* era a linear model depiction of innovation also applies, this time prioritizing the importance of market demand in driving innovation endeavors. What distinguishes this model from its predecessor is that rather than product development originating from scientific advances, new ideas originate in the marketplace, with R&D becoming reactive to these needs. The *third generation Interactive, Coupling or Chain-linked models* overcame many of the shortcomings of the previous linear atypical examples models, by incorporating interaction and feedback loops to recognize that innovation is characterized by a coupling of and interaction between science and technology and the marketplace. Consequently, the third generation models integrate multiple in-house functions and interdependent stages. While third generation models were non-linear with feedback loops, a sequential nature of the stages of innovation were characterized. In response, and aiming to reflect the high degree of cross functional integration within firms, *fourth generation integrated or parallel models* reflect 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. Extending from the previous generation of innovation models, *fifth generation systems integration and networking models* emphasize that innovation is a distributed networking process requiring continuous change occurring within and between firms, characterized 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 models are characterized 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. More recently and following

on from the seminal work of Rothwell's innovation generation model typology, researchers [23] have suggested that Chesbrough's [23] open innovation model represent the latest wave of innovation models. Reflecting a dominant orientation to the preceding network models of innovation, the open innovation approach is not limited to internal idea generation and development, as internal and external ideas in addition to internal and external paths to market (licensing, insourcing etc.) are facilitated within the innovation development chain.

In addition to the overarching innovation models, an extensive corpus of literature [6], [24], [7], [25] has accumulated documenting the range of end to end phases relating to innovation processes: idea generation, selection, development, implementation and launch, and post launch in some cases (as synthesized by [21]). A common thread emerging from the literature is that while there is logical order in these phases, the order is not necessarily linear. All models start with some form of idea generation or searching stage. Secondly, a selection phase follows to determine which projects are feasible and potentially lucrative enough to be pursued. Methodologies and practice of relevance to these initial stages include innovation management, market analysis and competitive intelligence, technology forecasting [25], [27], [28], [29]. The third step reflects the development phase where the idea is developed into a tangible product, process or service. This stage can be described differently where terminologies such as development, prototyping, manufacturing and realization are used interchangeably. Methodologies and practice of relevance to development stages include Agile, Lean Startup, Waterfall and Spiral [30], [31], [32], [33]. The fourth phase represents implementation/launch and typically entails marketing, distribution, logistics and customer facing activities. Business modelling and product road testing [34], [35] methodologies and practices offer significant contribution for this key stage. Some authors also include a post launch phase to accommodate re-innovating, scaling and learning dimensions [25], [8].

3.3 PACS Economics

As stressed by [36] 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. It is a notoriously difficult matter to estimate the cost and benefit components in the area of increased IT security and privacy. In a nutshell, the Economics of CyberSecurity and Privacy models IT security and privacy as decisions by the players involved. Mindful of this, the principles of economics to the analysis of cybersecurity and privacy opportunities/problems can provide insights into cost-benefit trade-offs faced by different market participants, their strategic behavior and market outcomes (i.e. welfare effects). At the core of the economics of cybersecurity and privacy are security risks. Especially important are financial gains as motivation for cybercrime. Moreover, the field also covers the analysis of market mechanisms and market failures as well as the economic impact of government regulations of cybersecurity. This field of research not only uses economic theory for the explanation of cyber security and privacy opportunities/problems, but also increasing-

ly employs approaches of behavioral economics. In this vain, cybersecurity and privacy issues can be evaluated using concepts such as asymmetric information problems (moral hazard, adverse selection) or externalities. The overview literatures typically concentrate on cybercrime statistics, market failures and instruments to improve market failures [37], [38].

The rationale for an economics perspective in this research is to surmount the difficulty of estimating tangible benefits leads to a problem of making a business case for spending on PACS. Often, companies only react with increased spending on IT security after a large-scale data breach has occurred. In such a situation, it is relatively easy for IT staff to make a business case. So timing is important for showing the value proposition of innovative PACS products and services. 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). If incentives are not aligned, they lead to suboptimal choices. For example, in order to obtain an economic incentive for the adoption of a new IT security system, the firm facing this decision needs to know (all) the costs and benefits involved in obtaining the system in order to make an optimal decision. There are a number of policy instruments that can impact on economic incentives of market players by changing cost-benefit categories and therefore the trade-offs of those participants. Mandatory instruments are implemented through legislation, regulations or mandatory Codes of Conduct encompassing: duty of care or diligence standards, Data breach notifications, property rights to personal information. Voluntary instruments include Trust marks and technical security seals i.e. TRUSTe, BBBOnline, EuroPrise; sharing of critical incidence information Computer Emergency Response Teams (CERTs) or Computer Security and Incident Response Team (CSIRTs). Other mechanisms are informal exchanges or community-driven Warning, Advice and Reporting Points (WARPs), the promotion of cyber insurance and security standards.

4 Guiding Principles for the IPACSO Framework

Responding to the challenge of transitioning technology related R&D into commercially viable innovations; the synthesis of the three aforementioned research streams signals a range of pertinent factors with reference to shaping the guiding innovation principles.

- Various market assessment techniques can support product development strategy at the “idea” level such as market hypothesis gathering, competitor and value chain assessments, product and technology roadmapping, business model generation and lean canvas techniques, and use case and persona development among others.
- Innovation process models involve a pattern of end-to-end stages and embody a diverse range of inter and intra stakeholders and processes. To offer tangible supports to PACS innovators, the proposed framework needs to accommodate each stage and support innovators in terms of their internal and external innovation ecosystems.

- Economic modelling of IT security and privacy purchasing decisions, market mechanisms and cost benefit trade-offs can inform business case, modelling and value propositioning supports.

Based on the foregoing triangulated desk research (discussed in section 3 above) and as listed below in Table 1, six preliminary innovation guiding principles have been formulated as a precursor to the overarching IPACSO framework to be developed.

Table 1. Derivation of the Guiding Principles

Research Themes	Guiding Principles	
PACS Market Analysis	1	Market Analysis: macro trends, technology SOTA, PESTEL, competitor analysis etc.
	2	Formulating Product/Service Idea: validation, scalability, value chain positioning, future proof etc.
Innovation Models	3	Innovation Process: identify/ refine /benchmark models, resourcing/ teaming/ incentivizing
	4	Innovation Training: ideation, development approaches, portfolio management etc.
PACS Economics	5	Legal/Regulatory/Standards Landscape: DP, CIO legislation, NIS Directive, CyberSecurity etc.
	6	Business Modelling: value propositioning, market validation, revenue sources, segmentation, channels etc.

These principles, transcending innovation process and training, idea formulation, market analysis, legal/standards landscape and business modelling categories integrates key focal points of relevance to innovation engagement and management. These building blocks represent the culmination of the first stage of the overarching IPACSO methodology, providing a synthesized helicopter overview of key considerations and potential menus/modules for the knowledge and decision-support innovation framework for identifying, assessing and exploiting market opportunities in the privacy and cybersecurity technology space. These preliminary guiding principles will form the underpinning inputs to the design of the IPACSO framework in terms of responding to, and meeting target stakeholders' innovation requirements, pain-points and needs. Importantly, these six focal areas represent a platform to refine existing innovation and market knowledge methodologies, practices and tools to support innovators in identifying, assessing and exploiting innovation opportunities These guiding principles will subsequently be validated via the IPACSO Innovation Advisory Board and extended outreach and dissemination channels and will inform the second stage

of the IPACSO process i.e. the development of the IPACSO Innovation Framework where knowledge paths and signposts to resources, tools and tactics will be provided to innovators to support their engagement, navigation and exploitation of their innovation endeavors.

5 Conclusions

The development of the proposed guiding principles represent a pivotal component in meeting IPACSO's overall goals of supporting increased awareness of innovation engagement and management practices, in addition to supporting greater awareness and knowledge of market dynamics, barriers and solution potential for increased innovation activity in the domain. The next phase in the IPACSO methodological process is to validate, and achieve consensus on these guiding principles through iterative stakeholder engagement in order to shape and inform the subsequent development criteria of the IPACSO framework. The actual components and content of the IPACSO framework will, in turn be developed into decision support modules and associated toolkits which will be equally iteratively developed, trialed and validated with target stakeholder engagement, primarily through validation training Bootcamps and wider dissemination and outreach channels.

Accordingly, the output of this initial phase of the IPACSO research project impacts and has implications at various levels, most notably in terms of framing both innovator and firm-level innovation requirements within the PACS domain, which has relevance to academic and policy making audiences also. Additionally, given that the research outputs form a pivotal component of the IPACSO project, they will actively contribute to ongoing debates and objectives around shaping support measures for PACS innovation awareness, competency building and innovation policy support developments in the domain. Furthermore, these insights, and the IPACSO project overall, will have relevance to the European trust and security Framework research programme portfolio which are increasingly charged with focusing on potential innovation arising from their activities, in terms of increasing project outputs for economic and societal benefit.

Bibliography

1 EC, "Cyber Security Strategy of the European union: An Open Safe and Secure Cyberspace," 2013.

2 D. Maughan, D. Baleson, U. Lindqvist and Z. Tudor, "Crossing the "Valley of Death": Transitioning Cybersecurity Research into Practice," *Journal IEES Security and Privacy*, vol. 11, no. 2, pp. 14-23, 2013.

3 OSMOSIS, "D2.1 Report on the Identified Security's Market Potential/ D2.2 Report on Taxonomy Definition," http://www.osmosisecurity.eu/system/files/OSMOSIS_D2.1%20and%20D2.2_integrated.pdf,

2010.

4 J. Tidd, "A Review of Innovation Models Discussion Paper 1," Science and Technology Policy Research Unit, Tanaka Business School, University of Sussex, 2006.

5 R. Garud, A. Kumaraswamy and V. Sambamurthy, "Emergent by Design: Performance and Transformation at Infosys Technologies," *Organizational Science*, vol. 1, no. 277, 2006.

6 R. Rothwell, "Towards the Fifth-Generation Innovation Process," *International Marketing Review*, vol. 11, no. 1, pp. 7-31, 1994.

7 K. Cormican and D. O'Sullivan, "Auditing Best Practice for Effective Product Innovation," *Technovation*, vol. 24, no. 10, pp. 819-829, 2004.

8 D. Jacobs and H. Snijders, "Innovation Routine: How Managers can Support Repeated Innovation," Stitching Management Studies, Van Gorcum, Assen, 2008.

9 G. Van der Panne, C. van Beers and A. Kleinknecht, "Success and Failure of Innovation: A Review of the Literature," *International Journal of Innovation Management*, vol. 7, no. 3, pp. 309-338, 2003.

10 N. du Preez and L. Louw, "A Framework for Managing the Innovation Process," in *PICMET Proceedings*, CapeTown, South Africa, 2008.

11 B. Jaruzelski, J. Loehr and R. Holman, "The Global 1000 Innovation Survey: Navigating the Digital Future," Strategy&PWC, http://www.strategyand.pwc.com/global/home/what-we-think/reports-white-papers/article-display/2013-global-innovation-1000-study, 2013.

12 Frost & Sullivan, " Global Cyber Security Market Assessment," February 17, 2014.

13 EC, "EU Data Protection Directive," http://ec.europa.eu/justice/data-protection/document/index_en.htm.

14 EC, "NIS Directive," http://europa.eu/rapid/press-release_IP-13-94_en.htm, 2013.

15 ITSEF IT Security Entrepreneurs Forum, "Discussion Roundtable," http://www.security-innovation.org/ITSEF.htm, 2013.

16 Forrester Tech Radar, "Data Security, Q2 2014," 2014.

17 Benzel, T.V, E. O'Brien, R. Rodriguez, W. Arbaugh and J. Sebes, "Crossing the Great Divide: From Research to Market," *Security & Privacy, IEEE*, vol. 11, no. 2, pp. 42-46, 2013.

18 Forrester Quick Take, "FireEye Acquires Mandiant," January 7th, 2014.

19 Tech Republic, "How Israel is rewriting the Future of Cybersecurity and Creating the Next Silicon Valley," 2013.

20 P. O'Raghallaigh, D. Sammon and C. Murphy, "A Re-Conceptualisation of Innovation Models to Support Decision Design," *Journal of Decision Systems*, vol. 20, no. 4, p. 369, 2011.

21 J. Ortt and P. van der Duin, "The Evolution of Innovation Management towards Contextual Innovation," *Euopean Journal of Innovation Management*, vol. 11, pp. 522-538, 2008.

22 M. Kotesmir and D. Meissner, "Conceptualizing the Innovation Process – trends and outloo," NRU HSE Working Paper Series "Science, Technology, Innovation". No.

10/STI/2013., 2013.

23 H. Chesborough, Open Innovation: The New Imperative for Creating and Profiting from Technology, Boston: Harvard Business School Press, 2003.

24 L. Dooley and D. O'Sullivan, "Structuring Innovation: a conceptual model and implementation methodology," *Enterprise and Innovation Management Studies,* vol. 2, no. 3, pp. 177-194, 2001.

25 J. Tidd and J. Bessant, Managing Innovation- Integrating Technology Market and Organizational Change, Chicester: John Wiley & Sons Limited, 2005.

26 C. Eleveens, , "Innovation Management; A Literature Review of Innovation Process Models and their Implications," Nijmegen, NL, 1-16, 2010.

27 R. Phal, C. Farrukh, and D. Probert, "Strategic roadmapping: a workshop-based approach for identifying and exploring innovation issues and opportunities," *Engineering Management Journal,* vol. 19, pp. 3-12, 2007.

28 R. Cooper, "Perspective: The Stage-Gate® Idea-to-Launch Process—Update, What's New, and NexGen Systems," *Journal of Product Innovation Management,* vol. 25, no. 3, pp. 213-232, 2008.

29 C.S. Fleischer, and B.E. Benoussan, Business and Competitive Analysis: Effective Application of New and Classic Methods, New Jersey: Financial Times Prentice Hall, 2007.

30 J. Highsmith and A. Cockburn, "Agile Software Development: The Business of Innovation," *Computer*, vol. 34, pp. 120-122, 2001.

31 E. Reis, The Lean Startup: How Today's Entrepreneurs use Continuous Innovation to Create Radically Successful Businesses, New York: Crown Business, 2011.

32 H. Takeuchi and I. Nonanka, "The New New Product Development Game," *Harvard Business Review,* Vols. January-February, 1986.

33 B. Boehm, "A Spiral Model of Software Development and Enhancement," in *Proceedings of an International Workshop on Software Process and Software Environments*, Coto de Caza, Trabuco Canyon, California, March 27-29, 1985., 1985.

34 A. Osterwalder and Y. Pigneur, Business Model Generation–A Handbook for Visionaires, Game Changers, and Challengers, New York: Wiley, 2010.

35 J. Mullins, The New Business Road Test, London: Financial Times/Prentice Hall, 2010.

36 L. Gordon, "Incentives for Improving Cyber security in the Private Sector: A Cost-Benefit Analysis", http://hsc-democrats.house.gov/SiteDocuments/20071031155020-22632.pdf, 2007.

37 T. Moore, "The Economics of Cyber Security: Principles and Policy Options," in *In Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.*, The National Academies Press, 2010., 2010.

38 T. Moore, R. Clayton and R. Anderson , "The Economics of Online Crime," *Journal of Economic Perspectives,* vol. 23, no. 3, pp. 3-20, 2009.