This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL REPORT

Security Challenges to the Use and Deployment of Disruptive Technologies

Neil Robinson, Maarten Botterman, Lorenzo Valeri, David Ortiz, Andreas Litgvoet, Rebecca Shoob, Eddy Nason

Prepared for the European Commission

RAND EUROPE

The research described in this paper was prepared for the European Commission. The opinions expressed in this study are those of the authors and do not necessarily reflect the views of the European Commission.

Published 2007 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
Westbrook Centre, Milton Road, Cambridge CB4 1YG, United Kingdom
RAND URL: http://www.rand.org/
RAND Europe URL: http://www.rand.org/randeurope
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Executive Summary

This report considers the security challenges to the use and deployment of disruptive technologies, which is a business and technology concept devised by Harvard professor Clayton M Christiansen. Disruptive technologies are those that sacrifice certain qualities in a product that are attractive to the majority of customers in favour of a different set of characteristics which may only be attractive to certain customers or which fulfil a certain specific niche need. Disruptive technologies or innovations are different from 'sustaining innovations'. Sustaining innovations maintain a constant rate of product improvement, leading to increasing functionality for the greatest number, or most profitable, customers. Disruptive technology can also create new markets by radically changing the market landscape, for instance, allowing new players to enter the market.

In trying to understand the security challenges associated with the use of these technologies, this report considers five specific disruptive technologies: Voice over Internet Protocol (VoIP); Radio Frequency Identification technology (RFID); Wireless Microwave Access (WiMAX); Trusted Computing and Internet Protocol version 6 (IPv6). Each technology was considered in the light of an implementation within an organisation, as a discrete case study.

To undertake the research, experts in Information Communications Technology (ICT) and information security were asked to participate in a Delphi exercise and workshop, where they rated their views on the security challenges to the deployment and use of the disruptive technologies. Overall, the research indicated that complex social and economic issues such as trust, risk and privacy were the most prevalent concerns. The experts also considered the business drivers for the implementation of these technologies, as security must always be seen in the light of hard-nosed business decisions. Following the classification of the different types of security challenges, the experts then helped in the design of a study framework that was used to guide the data collection for the case studies.

The case studies of the implementation of the five technologies were conducted in specific organisational settings. A combination of desk research, review of organisational documentation and first-hand interviews were used to collect the data, which was then reviewed and compared to other evidence.

The evidence showed that:

- The business case for the deployment of these disruptive technologies is not yet fully developed. As a result of this, the security considerations of the deployment

of these technologies may not be treated as seriously as they should, since these tend to be secondary to business concerns.

- Disruptive technologies present security challenges when organisations must transition from one version of the technology to another. These transitions must be properly managed if security is not to be undermined.
- The perception of the end user is an important issue, as it relates directly to usability and can also indicate how well the security message is understood.
- These technologies throw up reliability challenges; in particular as some of these technologies are key elements of the evolving European information infrastructure upon which governments, business and citizens increasingly rely.

On 30th June 2006, the European Commission and RAND Europe invited experts from industry, government and academia to Brussels to review the results of the case studies, express comment on the draft final report and debate the conclusions of the study at the Final Workshop. This event began with a presentation setting out the policy objectives and outlining the stages of the study, followed by an overview of the industrial and economic context (in particular, why it is important to study disruptive technologies and the market behaviours of disruptive technologies). An introduction to the study methodology was presented, and representatives from each of the case study organisations gave a short overview of their case study, reflecting: the general context of the deployment of the technology; business objectives and technical details of the implementation. Feedback provided during the workshop has been integrated in the conclusions and recommendations presented in this report.

In order to facilitate the successful treatment of these challenges, policy makers must adopt a supporting and encouraging role. The adoption of a disruptive technology is naturally self-regulated, spontaneous and 'bottom-up' due to the innovative and risky nature of these technologies. Policy makers in national governments and regional organisations such as the EU should not mandate that certain rules or standards are followed, or create overburdening laws that will hamper the dynamic growth of the single European Information Space. However, there is a role for targeted intervention in specific enabling areas, such as the implementation of IPv6 and legislation addressing issues such as privacy, data retention and monitoring.

This report makes the recommendations that governments should play a role where a societal benefit is expected, even if the market is not willing to pay for it. This role could be via: supporting pre-competitive research on the technology and its implementation and impact; regulating to reduce misuse and for certification; stimulation of standardisation and certification activities and awareness raising. Recognising that the successful and secure implementation of disruptive technologies requires the involvement of all stakeholders, policy makers should consider all likely market players, not just those with current market presence. Policy makers could define critical infrastructures and required minimum levels of operation, to better understand when specific regulatory or financial incentives are required to ensure their protection. In the context of the recently released strategy for a Secure Information Society: "Dialogue, Partnership and Empowerment" and the i2010 goals. We make recommendations to: ***inform*** all sectors at all levels about the security

challenges relating to these technologies and the policies in place to address them; ***stimulate*** good implementation by considering a coherent strategy for Europe-wide implementation of some of the technologies and by creating a positive regulatory environment to stimulate the development of new Ambient Intelligent infrastructures; ***integrate*** security in information systems to support prevention, for example by defining minimum levels of security or by using the buying power of the public sector; and finally ***implement*** risk assessment and protection mechanisms which could include improvements to law enforcement measures and laws. The report also presents specific policy recommendations for the European Commission, including: support of large scale demonstrators, exchange of good practice and standardisation, learning from industry good practice; ensuring avoidance of monocultures; providing continued support for pre-competitive Research and Development; improving education and training; and clarifying the legal implications of these new technologies.