Inclusive Information Society -

Challenges from a South African Rural Primary Healthcare Perspective

Dlamini, M.T.[1,2] & Eloff, J.H.P[1,2]
[1]SAP Research CEC Pretoria/Meraka Unit of Technology Development
[2]University of Pretoria
Department of Computer Science, ICSA Research Group
Pretoria, South Africa
{moses.dlamini; jan.eloff}@sap.com

Venter, E.[1] Smit, D.[1]
[1]SAP Research CEC Pretoria/Meraka Unit of Technology Development
Pretoria, South Africa
{el.venter; danie.smit}@sap.com

Abstract—**The European mandate for an inclusive information society is aimed at providing an environment that enables the billions of people who are at risk of exclusion at the "bottom of the pyramid" (BOP) to participate in an information society for all. Most organizations in Europe have realized that the fortune lies at the BOP. However, several challenges remain a stumbling block for those who want to exploit the opportunity at the BOP. This paper outlines such challenges looking at a rural South African primary healthcare context. The challenges described herein are "first-hand" experience and were encountered in a pilot project implemented in three rural primary healthcare clinics situated in the Mpumalanga province in South Africa. The paper concludes by providing recommendations on how to address the challenges in order to achieve a truly global information society that is fully inclusive.**

Keywords-Inclusive information society; bottom of the pyramid; information security; primary healthcare; rural communities

I. INTRODUCTION - INCLUSIVE INFORMATION SOCIETY

A common vision of an Inclusive Information Society was initiated at the 2003 world summit on the information society (WSIS) in Geneva [1]. At the summit, ICT was viewed as an essential foundation for an inclusive information society. As a follow-up on the above common vision, in 2006, ministers under the European Union (EU) signed the Riga Ministerial Declaration to declare their commitment to a number of concrete targets aimed at ICT for an Inclusive information society. These targets included: improving the Internet usage; digital literacy and skills; the availability and accessibility of ICT; and broadband coverage by at least 90% by 2010 [2]. This initiative was called the i2010 strategy; aimed at bringing onboard the groups of people at the risk of exclusion from an information society. With the Riga declaration, the ministers committed to turning the digital divide into a digital opportunity for all those who are at the risk of being excluded and further marginalized [1]. The mandate of the Riga declaration is to provide ICT for an inclusive information society to enable everyone to participate despite being societal or economical disadvantaged.

In an inclusive information society, ICT present the potential to ensure non-discriminatory access, bridge broadband and accessibility gaps, improve the quality of life of the disadvantaged people in rural areas, enhance the reach and impact of social development programs, and generate new local-community services [1]. ICT can also help in tapping the economic potential lying idle at the "bottom of the pyramid (BOP)" [3, 4].

The BOP is discussed in section II. The rest of the paper is structured as follows: section III discusses the gaps of the current initiatives towards an inclusive information society; section IV identifies the challenges in a South African rural primary healthcare context; section V provides recommendations and section VI concludes the paper.

II. BOTTOM OF THE PYRAMID

The BOP refers to the largest yet poorest socio-economic group that lives on less than $2 a day [4]. Paul Collier [5] refers to this group as the "Bottom Billion". This is the group that has been excluded and overlooked when it comes to an information society and economic activity. The BOP group has also remained invisible and unexplored by the corporate sector.

A. A Fortune At the bottom of the pyramid

The BOP group has been viewed as an untapped purchasing power with a large and lucrative market valued at $13 trillion [6, 7]. All off a sudden there is a fortune at the bottom of the pyramid [4] and corporate companies are rushing to seize the opportunity.

The average life expectancy is fifty years at the BOP compared to sixty seven years in developed countries and infant mortality is reported at 14% at the BOP as compared to 4% in developed countries [5]. The Riga mandate argues that ICT for an inclusive information society is expected to improve the quality of life of the underprivileged people at the BOP. Furthermore, this will open new and untapped markets for ICT technology providers.

The European Commission (EC) has proposed a strategic course of action to achieve the targets of the Riga mandate [3]. However, by the year 2007, there was still not enough progress made to meet most of the Riga targets. It is reported in [3] that this is due to fragmented efforts, lack of collaboration, unavailability or inaccessibility of ICT and

social differences in the use of ICT. Furthermore, the EU [3] reports the lack of trust, confidence and security in the use of ICT as additional challenges hindering a truly inclusive information society. This is despite the fact that security and trust have always been and will remain an important pillar on which an inclusive information society can be built. Security and trust builds confidence in the acceptance, adoption and usage of ICT by the marginalized people. Hence, the above are prerequisites for the development of an inclusive information society not only in the European context, but in the world-wide context and cannot be overlooked.

The EC has outlined a number of initiatives to address the above challenges in order to realize the Riga targets. These include an e-Inclusive awareness campaign, strategic framework for action; provide enabling conditions, legislative support, and coordination at the European level among others. The EC organized an annual conference that is dedicated to measure and monitor progress-made in achieving the EU's targets. The recent results show improvement in certain aspects like the roll-out of broadband and internet usage among others [8, 9]. This is however, not the case in developing countries.

III. INCLUSIVE INFORMATION SOCIETY - WHERE IS THE GAP?

In their quest to remain one step ahead, developed nations (EU) are continually failing to realize the global nature of an inclusive information society and they continue to work in silos leaving out the developing countries. Hence, there is no coordinated effort between developed and developing countries. Therefore, when considering a global context, there is still a lot that needs to be done to achieve an information society that is fully inclusive. It is very important for the developed and developing nations to cooperate both at regional and international level in order to fully realize a truly inclusive global information society.

There is a surging need to discuss the challenges of an inclusive information society both in developed and developing countries. This approach would provide a comprehensive picture of the steps that must be taken to achieve an inclusive global information society. This would also allow organizations to tap into the fortune that lies at the "bottom of the pyramid".

The main goal of this paper is to address the gaps that currently exist between developed and developing nations in terms of an inclusive information society. The discussions are mainly on issues surrounding the prerequisite for a truly inclusive information society in the context of rural South Africa as a developing country. The main research question is: how can we use ICT to tap the fortunes that lie at the BOP?

It is on this premise and in support of an inclusive information society, that SAP Research CEC Pretoria/Meraka Unit of Technology Development in collaboration with the University of Witwatersrand's School of Public Health and with the support of the Mpumalanga Provincial Department of Health along with other stakeholders embarked on a pilot project called PatHS (Patient Health System). In addition to the objectives of an inclusive information society, the objective of this pilot project is to develop a user-friendly patient health system for managing chronic diseases to improve primary healthcare in rural communities in South Africa [10, 11]. This pilot project took the initiative to work with the people at ground level to gain first-hand experience on their challenges. The main focus was on how ICT can be used to ensure that no one is left behind. The pilot project's core activities are centered on three primary healthcare clinics; i.e. Agincourt, Xanthia and Thokozani situated in the rural area of Bushbuckridge, South Africa. The following section presents the challenges that were encountered in the implementation of the PatHS pilot project. To fully reap the benefits of an inclusive information society, the following challenges in the next section must be addressed when it comes to a South African healthcare context.

IV. CHALLENGES

The following challenges were encountered in the PatHS pilot project and they are discussed in no particular order.

A. BorderlessCyberspace

"Hackers" in the underground know no international boundaries and distance is no obstacle. In the underground, there is no rural or urban, nor developing or developed countries; all computers that gets on the Internet becomes a fertile ground for malicious activity. As long as a computer is connected to the Internet and it does not have the necessary protection measures, it soon becomes vulnerable to information security threats. The risks are the same; whether the computer is located in rural Bushbuckridge in South Africa or urban Madrid in Spain. A worm that is meant to scan the Internet for computers with certain vulnerability will pick just about any computer with that vulnerability regardless of its geo-location. With this in mind, it does not matter that a system is implemented for first-time users in rural areas, the approach to information security should as vigilant as it would have been elsewhere in developed countries because attackers knows no boundaries.

However, the technical nature of security mechanisms makes it a big challenge to implement all the necessary security measures on systems to be used by first time users. First time users could easily get frustrated and stop using a system if every time they logon to do their work they are required to wait for at least 15 minutes while the system scan itself for viruses and other malware. Imagine a case where on every virus found the system waits for the user input on whether to clean, delete or quarantine the found virus before it could go on to scan other file. Considering the fact that first time users do not have the skills to bypass unnecessary steps, they could easily get frustrated and lose interest. This was the case in this pilot project, on the one hand you may want to secure the systems in the best way possible, but again you have to ensure that the security measures do not discourage the users from using the systems. This is very challenging especially when you still need the users to accept and adopt the system. A good example was when we disabled the USB ports to prevent the transmission of malware and the users discovered that the ports were not working and that negatively impacted their acceptance and confidence of the systems.

B. Very Low Wireless Broadband Penetration

The degree of penetration of fixed network infrastructure is relatively low in rural areas. The low coverage of fixed lines in rural areas can be attributed to their economic viability [12]. The market at the rural areas does not provide for sustainable economic return on an investment for fixed line infrastructure. Wireless broadband remains the only answer; however, the challenge in Bushbuckridge is that it is limited and unreliable. This may also be attributed to the area's economic viability. In Europe broadband coverage has reached the 100% penetration and now they are looking into ways of getting high-speed broadband [9]. In most developing countries like South Africa, we are still struggling to even get to 50% broadband penetration.

C. Lack of Digital Literacy

End-users are recognized as the most attractive target by "hackers" and they are increasingly at risk every time they connect to the Internet. Novice users for example those at the BOP are particularly likely to face difficulties in this context, as their unfamiliarity with ICT systems can limit their ability to recognize threats and understand the required protection. This was the case when the PatHS project was first implemented. The end-users first had to go through basic computer literacy training, before they could be introduced to the system. This was from point zero for most of the end-users as they had never used or touched a computer before. Basic security was introduced through the use of passwords and this was explained as similar to the case in bank cards with PIN (Personal Identification Number) not sharable. Passwords provide basic security and only when strong passwords are used. Furthermore, stealth information security threats can fool the best security experts, the situation is even worse for the novice users who have just been introduced to ICT with near zero threat awareness.

D. Security and Privacy

An inclusive information society depends on reliable security and it is everyone's responsibility to foster and build a secure cyberspace environment [13]. Insecure and untrustworthy ICT systems create a substantial risk more especially when considering the sensitivity and confidentiality of electronic medical records. The risk posed by insecure and untrustworthy systems in primary healthcare when electronic medical records are disclosed to unauthorized people carries severe consequences and has legal implications. Taking note of these we developed an information security policy tailored specifically to primary healthcare that the end-users would have to abide to.

We then provided physical security mechanisms for the systems both at storage and when in use. We also provided security mechanisms to protect the captured patient information, but the challenge was in ensuring that the end-users did not muddle with the system configurations and settings. There has been a lot of debate that security through obscurity is not good or dangerous [14, 15, 16, 17]. However, when faced with first-time users, we discovered that security through obscurity works well and the systems should be secure by default.

E. Unreliable Power-grid

At the beginning of the year 2008, Eskom (South African electricity supplier) implemented a series of scheduled electricity blackouts duped "load shedding". This was mainly because SA's power-grid could not cope with the load of power consumption from its customers. The demand for electricity exceeded the available supply. In order to manage the situation "load shedding" would be effected from time to time in certain areas [18]. Eskom tried to redeem the situation after the 2008 saga but their power-grid continues to be unreliable, more especially when you consider rural areas like Bushbuckridge. From time to time rural areas would go through an electricity blackout and it would take a long time before the problems would get addressed. By this time patients health information would be captured manually for entry when the systems come back on, a time consuming exercise for the nurses who are often under-staffed. This takes us to the next challenge we encountered.

F. Under-staffing

The one major problem facing primary healthcare in South Africa and the rest of the Southern Africa is that of under-staffing as nurses migrate to work in developed countries. It has been reported that South Africa has a serious and critical nurse shortage due to "brain drain" [19, 20]. This is even more pronounced when you take into consideration the misdistribution of the few health workers left between public vs private and urban vs rural areas. The problem of nurse shortage is worse in rural primary healthcare and as a result most rural primary healthcare workers are faced with an ever increasing workload. The case of a clinic cleaner who was found injecting children for immunization [19] shows just how deep this problem goes. In many instances, clinic clerks would be found performing healthcare workers' duties.

Lund & Flisher [20] reports a ratio of 19.5 healthcare workers per 100 000 population which is far less than appropriate and as compared to the case in developed countries. With this in mind, it is possible for patients to wait for days to get a chance to see a healthcare worker and they could possibly die before they could get that chance. The shortage of nurses contributes to a number of patient deaths that would have been otherwise avoided [21].

Evidently and as discussed in this section, the marginalized and underprivileged people at the BOP are faced with unique challenges. Therefore, it is of the utmost importance for any initiative that seeks to involve them to try and find appropriate solutions to address these challenges. If we can adequately address the current challenges, it would be very easy to move from the current status in rural primary healthcare as shown in fig. 1 to the futuristic scenario (of the Internet of Thing (IoT), Internet of Services (IoS) and Internet of People (IoP) leading to the IoPTS [22]) as shown in fig. 2.

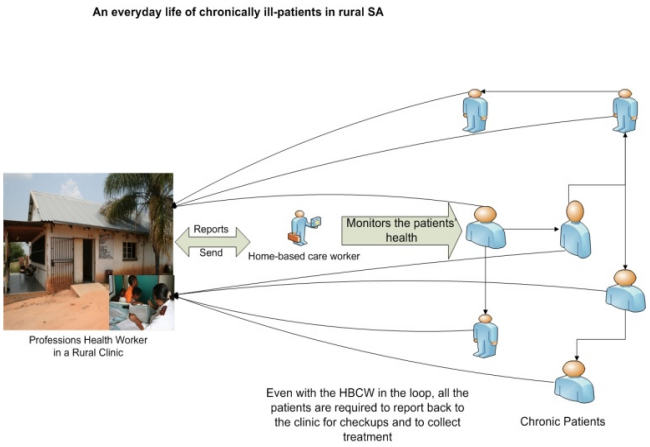

Figure 1. Current Status in rural primary healthcare

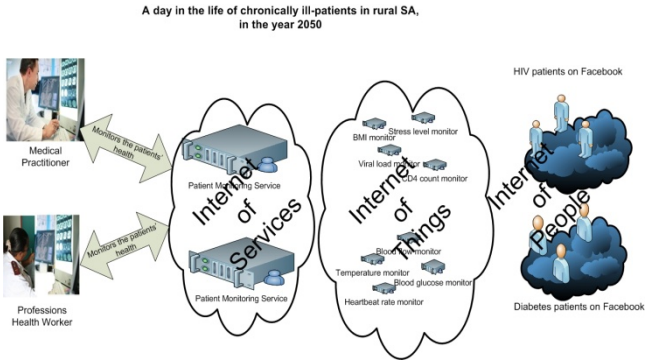

Figure 2. Futuristic scenario of a rural primary healthcare ()

V. RECOMMENDATIONS

In primary healthcare space, an inclusive information society would help in automating some of the processes like patient registration and patient file retrieval. This would in turn reduce the workload of the healthcare workers, ensuring that most of their time is spent on the patient's health problem rather than on administration. This will also improve the time lag to see a patient and hence increase the number of patients that get seen each day. Before taking a giant leap to embrace and implement the vision of an inclusive information society, it is very important to make sure that this is not a blind-folded leap towards a major catastrophe. This section provides some of the recommendations that could help in bringing the marginalized and underprivileged people in rural South Africa onboard to an inclusive information society without posing a major risk to either the data or ICT systems used.

A. *Provide Reliable Power-grid*

There is a great need improve the reliability of the power-grid in rural areas. Quite a number of times, when we carried out this pilot project power would go off and take hours to get it back. Providing backup batteries serve no purpose when power goes off for more than eight hours in a day. Eskom must do something to ensure that their power-grid is reliable and dependable because connectivity would be useless without electricity.

B. *Improve Connectivity*

Telecommunication companies have mentioned that rural areas are not economically viable for them to invest in. However, with all the focus now being shifted towards the BOP, it is time for telecommunication companies to reconsider the "untapped purchasing power" that lies at the BOP. Telecommunication companies like Telkom in South Africa must strive to improve their wireless broadband coverage and make it accessible, available, dependable and reliable. In addition they must deploy ICT systems that are capable of providing not just wireless broadband but provide high speed wireless broadband.

C. *Promote ICT Literacy and Skills*

Efforts must be made to promote ICT literacy and skills amongst the people at the BOP. The marginalized and underprivileged people in rural areas need to be educated and made aware of their responsibility for using ICT systems. Furthermore, they need to be trained on how to make the most of ICT systems and how they can best protect the data stored, processed and transmitted on their networks. The first-time users must be made aware of all the inherent risk involved when using ICT systems, not in a manner that will scare them away but in a manner that will inform and enlighten them.

D. *Strengthen Security and Privacy*

It is a duty of all medical practitioners to keep all patient health information confidential. The confidentiality of patient health information is governed by ethical rules of the medical profession, the constitution, national and international laws and regulations; all of which carries heavy penalties when a breached. On the other hand, financially motivated cyber-criminals know no boundaries. They target all vulnerable ICT systems that are connected to the Internet. This puts patient health information at an even higher risk.

Imagine an insurance company maliciously obtaining your medical records which shows that you suffer from the deadly HIV/AIDS virus. You would not stand a chance in getting an insurance policy with them. Even if you are lucky to get one, your monthly premiums will be very high forcing you to consider other options. Therefore, strengthening security and privacy is a prerequisite for preserving the confidentiality of patient health information in the healthcare space.

Secure and privacy preserving ICT systems builds confidence to the users and ensures better acceptance and adoption rates. ENISA [23] adds that security is a primary element for ensuring trust and confidence in electronic record and services that increasingly underpin critical aspects of our economy and an inclusive information society. Based on this, it is very important that ICT systems guarantee patient health data protection whilst at the same time respect the privacy of patient health information. The importance of international cooperation that will seek to foster and enhance a truly global culture of privacy and information security cannot be over-emphasized.

E. Increase the Numbers of Health Workers

The shortage of healthcare workers and their inequitable distribution is a cause of concern in South Africa [20]. The South African government needs to make sure that enough healthcare workers are trained in tertiary institutions to improve on the shortage that currently exists. The government also needs to ensure that healthcare workers are paid competitive salaries so as to avoid an "exodus". This is the most critical challenge that requires immediate attention from the current government if an inclusive information society is to materialize.

VI. CONCLUSION

The inclusive information society initiative is aimed at providing the billions of marginalized and underprivileged people at the bottom of the pyramid an opportunity to utilize ICT systems to improve their quality of life. In support of this aim is the South African initiative (the PatHS pilot project) that seek to provide the marginalized and underprivileged people of South Africa with ICT systems to improve healthcare service delivery at rural primary healthcare. This paper identified several challenges (i.e. *borderless cyberspace, very low broadband penetration, lack of digital literacy, security and privacy* among others) that must be addressed in order to achieve an inclusive information society. If these challenges are not addressed, it would be impossible to exploit the benefit of the pilot project i.e. the potential to help improve the quality of life of an average person living in SA's rural communities. Hence, this paper has outlined recommendations that would help facilitate a truly inclusive information society in the context of a South African rural primary healthcare.

ACKNOWLEDGMENT

The support of SAP Research CEC Pretoria/Meraka UTD and DEG towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at are those of the authors and cannot necessarily be attributed to SAP and DEG.

REFERENCES

[1] World Summit on the Information Society, "Building the Information Society: a global challenge in the new Millennium", Declaration of Principles, Document WSIS-03/GENEVA/DOC/4-E, 12 December 2003, available online: www.icsu.org/.../49_DD_FILE_Decl_of_Principles_12.12.03.pdf, [Accessed 13 May 2010].

[2] eInclusion@EU, "Strengthening eInclusion and Accssibility across Europe", eInclusion@EU Bulletin, No.2, 2006, available online: http://library.esangathan.eu/?p=37, [accessed 19 April 2010].

[3] Commision of the European Communities, "European i2010 Initiative on e-Inclusion: To be part of the Information Society", COM (2007) 694 Final, Brussels, 2007, available online: ec.europa.eu/.../einclusion/docs/...initiative/comm_native_com_2007_0694_f_en_acte.doc, [accessed 19 April 2010].

[4] C.K. Prahalad and S.L. Hart, "The Fortune at the Bottom of the Pyramid", Strategy + Business, No.26, pp. 1 – 14, 2002.

[5] P. Collier, "The Bottom Billion: Why the Poorest Countries are Failing and What Can Be Done About IT", Oxford University Press, USA, 2007

[6] A. Karnani, "The Bottom of the Pyramid Strategy for Poverty: A Failed Promise", United Nations, Department of Economic and Social Affairs (DESA) working paper No.80 ST/ESA/2009/DWP/80, August 2009.

[7] C.K. Prahalad, "The Fortune at the Bottom of the Pyramid: Eradicating Poverty through Profits", Wharton School Publishing, Upper Saddle River, USA, 2006.

[8] Council of the European Union, "Post-i2010 Strategy-Towards an Open, Green and Competitive Knowledge Society – Adoption of Coundil Conclusions", European Union, Brussels, 18 December 2009,available online: http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/trans/111999.pdf, [accessed 19 April 2010].

[9] Commision of the European Communities, "Europe's Digital Competitiveness Report Main Achievements of the i2010 Strategy 2005 -2009", COM(2009) 390 Final, European Union, Brussels, 4 August 2009, *available online:* ec.europa.eu/.../eeurope/i2010/docs/...report/.../com_2009_390_en.pdf, [accessed 13 May 2010].

[10] D Smit, E Venter, "Initial experiences from designing and implementing a clinical health information system in the primary healthcare sector of rural South Africa", IST Africa 2009, Kampala Uganda, April 2009.

[11] SAP AG, "SAP Research Report 2009/2010: From Creativity to Value", SAP Research Dissemination,2010.

[12] Y. Li, J.I. Agbinya, "Emerging Markets and Benefits of Fixed to Wireless Substitution in Africa," icmb, pp.605-609, International Conference on Mobile Business (ICMB'05), 2005.

[13] S. Ghernaouti-Hélie, "An Inclusive Information Society Needs a Global Approach of Information Security," ares, pp.658-662, 2009 International Conference on Availability, Reliability and Security, 2009.

[14] S.M. Bellovin and R. Bush, "Security Through Obscurity considered Dangerous", available online: http://www.cs.columbia.edu/~smb/papers/draft-ymbk-obscurity-00.txt, [accessed 12 May 2010].

[15] D. Owen, "In Defense of Security Through Obscurity", available online: http://danielowen.com/In_Defense_of_Security_Through_Obscurity, [accessed 12 May 2010].

[16] C. Perrin, "The Value of Accidental Security Through Obscurity", available online: http://blogs.techrepublic.com.com/security/?p=379, [accessed 12 May 2010].

[17] B. Schneier, "Schneier on Security: Security Through Obscurity Blog", available online: http://www.schneier.com/blog/archives/2008/06/security_throug_1.html, [accessed 12 may 2010].

[18] Eskom, "What is Load Shedding", Available online: http://www.eskom.co.za/live/content.php?Item_ID=5608, [accessed 19 April 2010].

[19] C. Zondagh, "Impact of Nurse Migration on Southern Africa", available online: http://74.125.77.132/search?q=cache:roN9PEb61CgJ:66.219.50.180/NR/rdonlyres/eniljbq4p6sta6i4mynlvhlnjmc5vbcd5x427y3yeyxwintjp3zko4ny6bxesn4wleelkt56eeyyjohcc5pyzhz2pmd/HP%25234.ppt+nurse-patiant+ratio+in+South+Africa&cd=6&hl=en&ct=clnk&gl=za, [accessed 19 April 2010].

[20] C. Lund and A.J. Flisher, "Staff/Population Ratios in South African Public Sector Mental Health Services," in South African Medical Journal, vol. 92, No.2, pp. 15 – 16, 2002.

[21] Solidarity Research Institute, "Nurse shortage in South Africa: Nurse/Patient Ratios Report", available online: http://www.unedsa.co.za/documents/Solidarity_Report_Nurse_shortage_in_SouthAfrica.pdf, [accessed 19 April 2010].

[22] J.H.P Eloff, M.M. Eloff, M.T. Dlamini and M.P. Zielinski, "Internet of People, Things and Services - The Convergence of Security, Trust and Privacy" Proceedings of the third International CompanionAble Workshop IoPTS, Brussels, 2 December 2009.

[23] ENISA, "i2010: A Strategy for a Secure Information Society", European Commision Information Society and Media, pp. 8 – 9, June 2006, available online: http://ec.europa.eu/information_society/doc/factsheets/008-esecurity-en.pdf, [accessed 13 May 2010