Exploring the Human Dimension in the Beneficiary Institutions of the SANReN Network

Y. Mjikeliso, J.F. Van Niekerk and K.L. Thomson

Institute for ICT Advancement, Port Elizabeth, South Africa
e-mail: {s209039445@; Johan.vanniekerk; Kerry-lynn.thomson}@nmmu.ac.za

Abstract

One of the factors that play a major role in information security is people. People are the drivers of most processes and procedures in information security. However, many researchers agree that human aspects are not given enough attention; more focus is given to the technical security. This is especially true in the security of the underlying network infrastructure which is often seen as a technical issue and not a human issue. It is senseless to have good solid technical security without considering humans because most security breaches are caused by human mistakes. Regardless of all the technical and physical controls implemented for network security, which underpins information security, there will always be human vulnerabilities to the security of the network. Therefore, attention should be given to the human factors as it is widely acknowledged as the biggest vulnerability in network security, which impacts on information security. In South Africa there is an important network infrastructure known as the South African National Research Network (SANReN) which provides vitally important Internet access to research and educational facilities throughout South Africa. The SANReN network has the potential to provide many opportunities and benefits to the people of South Africa. It is therefore extremely important that the SANReN network is highly secured at all times in order to ensure continued availability of the network. This paper will focus on human factors that could affect the security of the SANReN beneficiary networks. Policies governing the use of the SANReN network will be investigated in order to establish whether human factors, which could pose security risks to the SANReN network, have been addressed in the policies.

Keywords

Human Factors, SANReN Beneficiary Networks, Policies

1. Introduction

The management of information security depends on technology, processes and people. However, more emphasis is often placed on strengthening the technological aspects and processes, while less attention is given to the human aspects (Ashenden, 2008). Even security surveys commonly acknowledge that the human aspects, such as policy, training and education, are more likely to be given less attention than the technical controls, such as firewalls, antivirus and intrusion detection (Furnell & Clarke, 2012). Regardless of all the technical and physical controls implemented for network security, which underpins information security, there will always be human vulnerabilities to the security of the network. Information security is about the protection of information and its critical characteristics (confidentiality, integrity, availability), as well as the systems and hardware that use, store and transit that information (Whitman & Mattord, 2011). Network security is one underlying component of information security without which it may be difficult to achieve information security. This paper will firstly determine whether human factors are considered or addressed in the security of the SANReN beneficiary networks. The paper presents content analysis of the existing policies used to govern the SANReN network, in order to determine whether human factors which could affect the security of the SANReN network have been addressed in the policies.

2. Methodology

The paper utilises a combination of content analysis of policies, as well as interviews with SANReN network engineers and a network administrator from one of the SANReN beneficiary institutions. All current policies governing the SANReN network were gathered by collecting documents from the TENET (discussed in Section 2.2) website, through email correspondence with SANReN personnel, as well as through interviews with network administrators at beneficiary institutions. The main focus of the content analysis of the policies was to identify whether or not human factors or human aspect issues were currently being addressed within the SANReN policies.

3. NREN

A National Research and Education Network (NREN) is a specialised Internet service provider for the research and educational communities within a country (TERENA, 2010). It provides research institutions and educational institutions with services and access to the Internet. Other than just providing connectivity to the Internet, the NREN should also provide a number of important services such as a Network Operations Centre, performance monitoring and management, incident response (TERENA, 2009). The way in which the NRENs are managed from country to country differs, as the organizational and ownership model for each NREN varies (TERENA, 2010).

3.1. SANReN

SANReN is a high speed communication network that is designed primarily for research institutions and organizations. The main purpose of the SANReN network is to provide the South African research institutions and organizations with Internet access and related services, as well as connecting them to research networks all over the world. The SANReN network together with the Centre for High Performance Computing (CHPC) and Very Large Databases (VLDB) create the key components of the cyber infrastructure in South Africa (Meraka Institute, 2007). The major role players of the SANReN network are:

- Department of Science and Technology (DST)
- Council for Science and Industrial Research (CSIR) Meraka Institute
- Tertiary Education and Research Network of South Africa (TENET)
- SANReN beneficiary institutions

The SANReN network is a South African DST project, implemented by the CSIR through the Meraka Institute (Meraka Institute, 2007). The project is part of the South African government's approach to cyber infrastructure to ensure the successful participation of South African researchers in global knowledge (SANReN, 2014). The CSIR is the governing body of the SANReN network and the operational services of the SANReN network to all beneficiary institutions is provided by TENET on behalf of the CSIR (SANReN, 2014). A *beneficiary institution* is an institution that is defined by the DST as institutions that are allowed to be connected to the SANReN network. These beneficiary institutions are the current TENET institutions, such as universities and research councils (SANReN, 2014). The following subsection will provide more detail on TENET which is one of the SANReN role players.

3.2. TENET

TENET is a specialized ISP for higher education and research sector, which provides Research and Education Networking services "REN services" like Internet and related services to about 160 campuses of 54 institutions, including universities, research councils and other associated institutions (UbuntuNet Alliance, n.d.). All the public universities and science councils in South Africa qualify to be a part, or a member, of the TENET network (Martin, 2012). The South African NREN is formed by SANReN together with TENET. The roles and responsibility of the South African NREN (SANReN) are given to both the SANReN team and to the TENET team. The SANReN team build the network and the TENET team operates the network (Martin, 2012). The following subsection will focus on how the SANReN network is being rolled out.

3.3. SANReN Network Implementation

The SANReN project is being rolled out in a phased manner and will eventually connect up to 204 sites across South Africa, and connecting over 3 000 education and research organizations from all over the world (SANReN, 2014). The South African universities, research councils such as the CSIR, National Research Foundation (NRF) , and various other research institutes are the beneficiary institutions of SANReN (SANReN, 2014). These beneficiary institutions form the SANReN national network backbone. The SANReN network backbone consists of a 10Gpbs 7-stretch backbone ring between the South African major cities. The SANReN Point of Presences (PoPs), are placed in all the connected institutions. The rolling-out of SANReN is still progressing to other beneficiary institutions and will eventually also connect remote towns (Martin, 2012). SANReN has the potential to provide many opportunities and benefits to the people of South Africa. Rural areas will have increased accessibility to the Internet, which could help in addressing the digital divide (SANReN, 2012). The SANReN network is one of the cyber infrastructures attempting to close the digital gap between those who have access to the Internet and those who do not have, and will connect a wide variety of people. Therefore, it is important that the SANReN network is secured at all times in order to ensure the continued availability of the network.

4. Securing the SANReN Network

Many NRENs have Computer Security Incident Response Teams (CSIRTs) in place in order to respond to security incidents of the network (Moller, 2007). As a result, the SANReN team is also in the process of establishing a SANReN / TENET CSIRT team which will be responsible for managing the security incidents of the SANReN network. CSIRT is a team of people who are responsible for receiving and responding to network security incident reports and activities (Mooi, 2013). The need for the SANReN / TENET CSIRT was identified through a survey conducted in May 2012 (Mooi, 2012a). The survey was sent out to all the beneficiary institutions of the SANReN network. The purpose of the survey was to investigate whether the beneficiary institutions would be interested in an incident response team, as there is no central point, or a central managing party, for incident handling on the SANReN network at present. The TENET NOC (Network Operations Centre) is responsible for incident handling. However, there may be restricted resources and the TENET team may lack effectiveness since they may be the only ones responsible for incident handling (Mooi, 2012a). When the SANReN / TENET CSIRT team is established it will be responsible for protecting against all types of malicious activities on the SANReN network such as; spam, denial of service attacks or hacking attempts. Their responsibility will be to receive, review and respond to the network security incidents (Mooi, 2012b). From a technical point of view, the SANReN network may be more secure as a result of the SANReN / TENET CSIRT team. However technical controls should not be the only concern for addressing security on the SANReN network – human factors should also be of concern, as will be discussed in section 4. The SANReN network may be vulnerable to risks posed by human factors even if technological controls exist on the network.

5. Human Factors on the SANReN Network

"Don't rely on network safeguards and firewalls to protect your information. Look to your most vulnerable spot. You'll usually find that vulnerability lies in your people" (Mitnick & Simon, 2002). There are technical solutions for solving what is seen as a technical issue. However, having technical solutions can create a false perception of security. Even though technical security is very important and without it networks would be vulnerable, there is still a vulnerability that remains because of negligence and the malicious acts of human beings. Negligence, ignorance, anger or even curiosity are human elements which can increase security incidents (PricewaterhouseCoopers, 2010). Human beings are a more challenging problem to address because there is no easy way to target them; there are no product-based solutions for people, unlike technical solutions (Furnell & Clarke, 2012).

Many researchers agree that human factors are one of the most significant vulnerabilities in information security and are often overlooked in organizations (Thomson & von Solms, 2006; Kraemer & Carayon, 2007). People are said to be the greatest threat to information security, and are often the 'point of failure', whether intentionally or through negligence or a lack of knowledge. However, people could represent the key element in achieving security (van Niekerk & von Solms, 2010;

Furnell & Clarke, 2012).Human factors play a role on the SANReN network just like in any other network. The rolling out of the SANReN network has started for various beneficiary institutions and a number of people have been involved with this project. There are people involved in configuring the network devices, creating policies and using the network as end-users. It is important to understand that, by nature, people have limited attention and accuracy - they make mistakes and errors (Ashton, 2009). Therefore, SANReN must properly address the human vulnerabilities. The mistakes and errors that people make could result in security vulnerabilities (Kraemer, Carayon, & Clem, 2009). The greatest vulnerability to the security of the SANReN network may be the people that the network connects or the employees.

An interview was conducted with one of the network administrators at the Nelson Mandela Metropolitan University (NMMU), which is a beneficiary institution of the SANReN network. The interview was conducted in order to identify whether issues related to human factors could pose security risks to the SANReN network. The network administrator was completely certain and confident about the technical and physical security of SANReN network. "We believe that the management of SANReN is being done by some of the best IT professionals in South Africa, so in my opinion, I believe that the network configuration is as secure as necessary". According to the network administrator, the beneficiary institutions host the network devices and the TENET team remotely accesses the devices or sends someone from SANReN / TENET when they need to make configuration changes on the network devices. There are no people working for SANReN / TENET at the beneficiary institutions and the connected institutions have no management or configuration access to the SANReN networking devices. However, the network administrator also mentioned an incident where on one or two occasions the SANReN network administrators from TENET managed to lock themselves out of the remote configuration session. They required local assistance from IT staff at the NMMU and the local IT staff had to make the configuration changes to the network device of SANReN. The fact that the TENET people were able to lock themselves out of the configuration session indicates there was a human mistake or error. Therefore, through this human error, members of the local IT staff at the NMMU were given access to network devices that they should not usually have access to. From this incident it could be implied that even though the network might be seen as technically and physically secured, human factors could be the weakest link in the security of the SANReN network.

For example, here in South Africa there are institutions from disadvantaged areas which might lack highly trained IT professionals. What if a low-level skilled individual was asked to perform these changes on the SANReN network devices and ended up misconfiguring the devices creating more problems on the network? Having been granted access to the networking devices and, for example, knowingly or unknowingly connecting a device which contains viruses and worms which may be distributed throughout the network could have a severe impact on network security. Therefore, the SANReN / TENET network may be exposed to many security risks by allowing access to the wrong individuals. SANReN / TENET are not aware of how skilled or qualified the individuals are that they are giving access to the network. This may present a good opportunity for an insider threat to manifest. An insider threat poses a security risk to the network because of the legitimate access to facilities, information, and knowledge of an organization and the location of valuable assets (Williams, 2008).

Another possible threat would be to apply a security related patch to incorrect software or failure to secure the correct port making it a target for network attackers. Most network attackers usually start by looking for vulnerabilities or weaknesses of the individual or computer they can communicate with on the network targeted. Many software packages will never be free of vulnerabilities because of human errors (Grobler & Bryk, 2010). Any network will have some level of vulnerabilities as it is impossible to completely eliminate vulnerabilities (Ritchey & Ammann, 2000). It is, therefore, very important that networks such as SANReN properly address the vulnerability of human factors. In other words, their end-users and IT staff must know their roles and responsibilities and adhere to correct behaviour to protect the network. In order for people to adhere to correct behaviour there must be organizational policies from management dictating the appropriate behaviour of the employees (von Solms & von Solms, 2004). As mentioned previously, information security, to a large extent, relies on the security of the underlying infrastructure or network. The management direction, rules, regulations and procedures regarding the protection of information assets must be part of an information security policy. In order to change or influence the behaviours of people in an organization the information security policy and procedures must be properly communicated to all parties, such as employees of the organization and business partners (von Solms & von Solms, 2004). Employees of an organization would, of course, include IT staff. People could be the greatest threat to information security, and the related network security especially if policies, education, training and awareness are not properly utilized to prevent people from accidentally or intentionally posing risks to the security of network (Whitman & Mattord, 2011). Vulnerabilities may come from employees who do not comply with information security policies (Siponen, Mahmood, & Pahnila, 2014). Therefore, it is important that organizations like SANReN have policies in place in order to dictate the appropriate employee behaviour and better control what people can and cannot do on the network or network devices.

An investigation into the existing policies which manage the use of the SANReN network was conducted. The authors consulted appropriate people from SANReN concerning the current policies between SANReN and the SANReN beneficiary institutions. The authors were directed to the TENET website where the policies between SANReN and the beneficiary institutions were located. From the policies the authors were specifically looking for the operational roles and responsibilities of people in the SANReN network. The following questions were used to focus the content analysis of the TENET policies:

1. Who is allowed to have physical access to the SANReN devices of the beneficiary institutions?
2. Who can configure SANReN devices in the beneficiary institutions?

3. What minimum skills or qualifications should the people who configure SANReN devices in the beneficiary institutions have?
4. Are there training programs or some form of education that is given to the beneficiary institutions connected to the SANReN network?

The following policies were examined in order to determine whether human related issues regarding the previous questions have been addressed in the TENET policies. These policies were the only ones that existed on the website and according to the people of SANReN these policies are the only ones in existence that currently govern the use of the SANReN network: Acceptable Use Policy (AUP), Connection Policy and Privacy Policy. All these policies are created by TENET as it is the operating entity of the SANReN network. These policies are to the authors' knowledge the only ones that manage the use of the SANReN network. An analysis of these three policies was done in order to identify whether human factors are addressed in the policies and will be discussed in the following subsections.

5.1. Acceptable Use Policy (AUP)

The purpose of the TENET AUP is to outline for the SANREN beneficiary institutions the things allowed and not allowed on the network. It defines rules and responsibilities of the SANReN beneficiaries or participating institutions. According to the TENET AUP the beneficiary institutions are allowed to use the REN services for any legal activity which furthers the goals and aims of the institution, and only if their activity does not include any unacceptable uses. If the beneficiary institution does what is unacceptable on the network, the provision of the REN services may be discontinued by TENET. A few of the unacceptable uses of the REN services that are listed on TENET AUP are:

"Any attempt to use the REN services in a way that breaches or would breach the security of another user's account or that gains or would gain access to any other person's computer, software, or data or otherwise threaten another person's privacy, without the knowledge and consent of such person"

"Any failure to secure a server that is connected via the REN services to the Internet against being abused by third parties as an open relay or open proxy"

"Any effort to use the REN services in a way that circumvents or would circumvent the user authentication or security of any host, network account ("cracking or hacking")"

These are some of the unacceptable uses of the REN services which are listed in the TENET AUP. With regard to the questions posed previously, the TENET AUP stated nothing regarding physical access to SANReN devices in beneficiary institutions. Nothing was stated regarding people who are allowed to configure the SANReN devices. There was nothing stated about the level of skills or qualifications of people configuring SANReN devices in the beneficiary institutions and there was nothing mentioned regarding any form of training program which may be provided to beneficiary institutions by SANReN / TENET.

5.2. Connection Policy

The Connection Policy lists all types of connections which are available when connecting a Research and Education Network (REN). This policy specifies the differences, rules and responsibility of each connection. The REN network connection types are; direct on-site connection, direct PoP connection and indirect connection. The direct on-site connection is a type of connection which is under TENET operational management where the hand-off location is at the connecting site not the connecting party (beneficiary institutions). Hand-off location is the point where operational responsibility changes between the beneficiary institution and TENET (TENET, 2014). For the direct PoP connection the hand-off location is at the Point of Presence and TENET does not operate the terminating equipment at the connecting site and does not operate the access circuit between the connecting site and PoP. The institutions which have direct connection can then provide an indirect connection to other smaller research and education organizations around them. Places such as education and training colleges, schools and public museums can connect to the beneficiary institution’s direct connection in order to access the REN services. However, the indirect connection is the responsibility of the SANReN beneficiary institution that connects it not of TENET. With regard to the questions previously posed, the TENET Connection Policy does not mention anything regarding physical access to SANReN devices in beneficiary institutions and nothing was mentioned about configuring devices. There was nothing stated about the level of skills or qualifications of people configuring SANReN devices in the beneficiary institutions and there was nothing mentioned regarding any form of training program which may be provided to beneficiary institutions by SANReN / TENET.

5.3. Privacy Policy

The TENET Privacy Policy explains how the personal information which TENET collects from TENETs contacts is used. TENET contacts are the people who work with TENET, such as the representatives of the beneficiary institutions, suppliers and other contractors (TENET, 2014). The TENET Privacy Policy states that TENET respects the privacy of its contacts and will protect the confidentiality of the contacts’ personal information. With regard to the questions previously posed, the TENET Privacy Policy does not state anything regarding the physical access to SANReN devices in beneficiary institutions and nothing was mentioned regarding people who are allowed to configure devices. There was nothing stated regarding the level of skills or qualification of people configuring SANReN devices in the beneficiary institutions and there was nothing mentioned regarding any form of training program which may be provided to the beneficiary institutions by SANReN / TENET.

After conducting the analysis of the TENET policies, it can be noted that the AUP, Connection Policy and the Privacy Policy do not adequately address the human factors which might pose risks to the security of the SANReN network. None of the policies state the operational roles, responsibilities and procedures on the SANReN network. There was no documented framework that deals with security vulnerabilities posed by the human factors on the SANReN network and no clear guidelines and procedures concerning things like access control and authorisation. There was nothing mentioned about accessing the network devices nor about locking the doors or monitoring the room where these devices are placed. In other words, there were no direct rules and responsibilities or operational procedures addressed in these policies. If there are no proper procedures which people can abide by, the security of the network may be at risk. It may make it easier for unauthorized individual to gain access to the devices and, intentionally or unintentionally misconfigure network devices. Once an unauthorized person gains access to the devices even the technical solutions will not help in protecting the network. It is, therefore, very important that a security policy addressing operational concerns, for example, an operational security policy is put in place in the SANReN network and enforced in all the beneficiary institutions. Policies which outline the responsibilities and roles of people in the beneficiary institutions should be in place to better secure and manage the SANReN network. There is definitely a need for a formalized approach such as a framework or guidelines for addressing human related behaviour on the SANReN network.

6. Conclusion

This paper examined the existing policies which govern the use of the SANReN network. The TENET policies were examined to determine whether the issues of human factors, which could threaten the security of the SANReN network, were adequately addressed. The paper outlined that there were no current policies which address human factors on the SANReN network. Therefore a formalized approach to addressing human factors in the SANReN network is recommended as human factors could be the greatest risk to the security of the network. Just as there are formal policies in place to govern the use of technical controls, there should also be formalized policies in place to address human factors in order to strengthen the security of the SANReN network. Formal documents, such as an operational security policy, outlining the roles and the responsibilities of people involved in governing the SANReN network should be created and enforced in the SANReN beneficiary institutions. These policies should address all possible human related security concerns, ranging from Bring Your Own Device (BYOD) policies to security awareness and training. Future research would include creating a framework or guidelines which will address human factors in the SANReN network. The framework or guidelines could address issues such as the identification of role players and their responsibilities, determination of skills and the provision of a formalized training program to the beneficiary institutions.

7. References

Ashenden, D. (2008). Information Security management: A human challenge?, *13*(4), 195–201.

Ashton, K. (2009). That'Internet of Things'Thing. *RFID*. Retrieved from http://www.rfidjournal.com/articles/view?4986

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983–988. doi:10.1016/j.cose.2012.08.004

Grobler, M., & Bryk, H. (2010). Common Challenges Faced During the Establishment of a CSIRT. *IEEE*, 2–7.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists., *38*(2), 143–54.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, *28*(7), 509–520. doi:10.1016/j.cose.2009.04.006

Martin, D. (2012). *Tertiary Education and Research Network of South Africa NPC* (pp. 1–4). Retrieved from http://www.tenet.ac.za

Meraka Institute. (2007). African Advanced Institute for Information and Communication Technology. Retrieved from http://www.meraka.org.za/Faqs

Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception*. (C. Long, N. Stevenson, & J. Atkins, Eds.). Robert Ipsen.

Moller, K. (2007). Setting up a Grid-CERT : experiences of an academic CSIRT, *24*. doi:10.1108/10650740710834644

Mooi, R. (2012a). *Security Incident Response for the South African NREN* (p. 9). Retrieved from http://www.sanren.ac.za/wp-content/uploads/2012/11/IRT_background_survey_problem_SANReN.pdf

Mooi, R. (2012b). *Introduction to CSIRTs* (p. 5). Retrieved from http://www.sanren.ac.za/wp-content/uploads/2012/11/SANReN_CSIRT_Introduction.pdf

Mooi, R. (2013). *SA NREN CSIRC Model* (p. 14). Retrieved from http://www.sanren.ac.za/wp-content/uploads/2013/05/SA_NREN_CSIRC_Model-Published.pdf

Networking in South Africa.pdf. (n.d.).

PricewaterhouseCoopers. (2010). *Protecting your business*. *Veterinary Record* (Vol. 122). doi:10.1136/vr.122.17.421

Ritchey, R. W., & Ammann, P. (2000). Using Model Checking to Analyze Network Vulnerabilities. *IEEE*.

SANReN. (2012). *About SANReN* (pp. 1–11).

SANReN. (2014). SANReN Overview. Retrieved April 10, 2013, from http://www.sanren.ac.za/overview

Siponen, M., Mahmood, A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217–224. doi:10.1016/j.im.2013.08.006

TENET. (2014). TENET Standard Terms and Conditions. Retrieved January 22, 2014, from http://www.tenet.ac.za

TERENA. (2009). *TERENA COMPENDIUM*. Retrieved from www.terena.org/compendium

TERENA. (2010). Research and education networking FAQ. Retrieved from http://www.terena.org/activities/

TERENA. (2013). *TERENA COMPENDIUM*.

Thomson, K. L., & Von Solms, R. (2006). Towards an Information Security Competence Maturity Model. *Computer Fraud & Security*, 11–15.

UbuntuNet Alliance. (n.d.). TENET South Afrca. Retrieved from www.ubuntunet.net

UbuntuNet Alliance. (2013). *What is UbuntuNet?* Retrieved from www.ubuntunet.net

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective, *29*(4), 476–486.

Von Solms, R., & Von Solms, B. (2004). From policies to culture. *Computers & Security*, *23*(4), 275–279. doi:10.1016/j.cose.2004.01.013

Whitman, M., & Mattord, H. (2011). *Principles of Information Security*.

Williams, P. A. H. (2008). In a “trusting” environment, everyone is responsible for information security, *13*(4), 207–215.