Strategic Information Security: Facing the Cyber Impact

Marthie Grobler
Council for Scientific and Industrial Research, Pretoria, South Africa
mgrobler1@csir.co.za

Abstract: Strategic information security is becoming a more prominent aspect of modern day living. With the strong digital component that forms part of modern day business, the multiplicity of security risks and the emergence of increasingly complex threats necessitate an integrated organisational approach to information security. However, the best information security infrastructure cannot guarantee that cyber attacks and malicious intrusions will not happen. It has become necessary to face the impact of the cyber realities by knowing the facts and understanding the direction of cyber trends and threats beforehand. This is strongly supported by the proactive use of forensic readiness as part of the information security strategy.

Keywords: Cyber threat, Cyber trend, Information security, Proactive, Strategy.

1. Introduction

"The success of the Internet has not only changed how the world does business, it also has transformed forever the nature of the risks that organisations face" [17]. No longer is it a viable option for organisations to react only once an information security risk emerges. It has become eminent for organisations to know their environments, to anticipate any information security risks beforehand, and to face the cyber impact proactively as part of the organisational strategic plan.

With the strong digital component that forms part of modern day business, the multiplicity of security risks and the emergence of increasingly complex threats necessitate an integrated organisational approach to information security. The best information security infrastructure, however, cannot guarantee that cyber attacks and malicious intrusions will not happen. It has become necessary to face the impact of the cyber realities by knowing the facts and understanding the direction of the cyber trends and threats beforehand. This, supported by the proactive use of forensic readiness as part of the information security strategy, will ensure a practical, cross-functional approach for using security to enhance competitiveness of an organisation [17].

Strategic information security can be defined as: *the process of identifying and effectively mitigating or managing any developments that may threaten the resilience and continued survival of a corporation, at an early stage*. It oversees and manages the close coordination of all functions within the company that are concerned with security, continuity and safety. In order to ensure strategic information security, this article introduces the impact of the cyber reality by addressing current cyber trends and threats in Africa. It further proposes forensic readiness as proactive measure to ensure strategic information security. The article concludes with a mapping of the cyber impact and forensic readiness actions on the definition of strategic information security, presented in Table 1.

2. Current cyber trends and threats in Africa

A division of Symantec Corporation undertook an enterprise security survey in January 2010. The respondents came from small, medium and large enterprises from across 27 countries, reaching about 2100 individuals. Most of the respondents included Chief Information Officers, Chief Information Security Officers and senior Information Technology management. The report indicates that 42% of organisations ranked cyber security as their top risk, outranking traditional crime (17%), natural disasters (17%) and terrorism (10%) [23].

This statistic places cyber and information security as a significant aspect of concern for a number of organisations. With cyber security heading the list of significant organisational risk, a lot of attention needs to be given to cyber space trends and threats. Therefore, it is necessary to maintain a current awareness of trends and threats to facilitate a proper understanding of the cyber impact.

2.1 Cyber trends

Cyber attackers are increasingly becoming more sophisticated in their attack strategies and techniques. Cyber trends can thus be defined as the long-term movement and general direction in which cyber activities move.

2.1.1 Trend 1: Internet penetration

"Nine in 10 South Africans are still not online, with many in poor townships or rural areas relying on internet cafes or doing without" [21]. According to Internet World Stats [11], the number of African internet users is 991,002,342 (estimation based on December 2009 figures). Although this figure shows a user growth of 1,809.8% since 2000, it translates to a penetration percentage of only 8.7%. This means that only about 113,908,315 Africans have access to the internet. Figure 1 shows the global internet penetration graphically. The darker shaded areas represent the highest internet penetration, whilst the lighter shaded areas represent the lowest internet penetration.

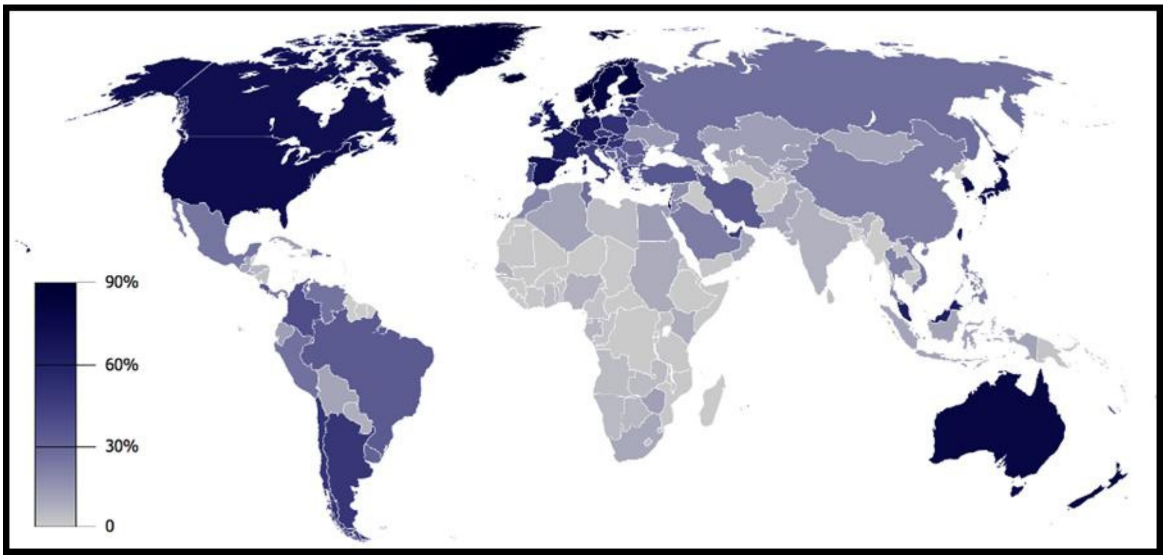


Figure 1: Global internet penetration [1]

According to Otieno [18], Africa has the lowest number of internet users in the world. Regardless, the recent rapid growth of African internet users due to the broadband rollout project may be the catalyst of numerous threats to cyber space. Egypt represents most of Africa's internet users with 12.6 million people participating on the internet, followed by Nigeria with 11 million people, Morocco with 10.3 million people, South Africa with 5.3 million and Sudan with 3.8 million people [11] [18] [21]. Although only 8.7% of the African population have internet access, it means there are still 113,908,315 people that are potentially vulnerable to cyber attacks. The magnitude of African internet users may leave the African internet vulnerable to cyber attacks. This in turn may have a negative impact on the South African information security, in the case that the African network comes under cyber attack.

2.1.2 Trend 2: Bandwidth availability

Until recently, slow and expensive download times in Africa was a reality. South African internet users were to some extent inherently risk proofed. For example, the daily update of new virus definitions from Symantec is around 40MB and McAfee's is around 100MB. On a 56Kb dialup link, this can take all day to download [13] and might dissuade individuals from downloading. From a business point of view, slower internet speeds also equate risk proofing against digital theft. *"Over a slow Internet link, it might have taken days to transfer even one 1GB of stolen data, but with fibre optics, the same can happen in minutes. Generally, the faster the link, the higher the amount of threats that might come"* [6].

To address the availability of bandwidth within the African continent, France Telecom-Orange signed a memorandum of understanding in November 2008 to install a submarine fibre optic cable that will provide internet access to over 20 countries within the West African coastal region. Although the project is not yet completed, the Seacom cables already provide fast broadband access to a number of South Africans, linking the South African coast with Europe [21]. The increased broadband usage creates a favourable environment for increased cyber space criminal activities. Not only are there potentially more victims, but the technology is faster, allowing more virus distributions and infections [8].

2.1.3 Trend 3: Bandwidth cost

In general, high internet prices are due to the reliance on satellite connectivity. On average, accessing the internet costs Africans 50-100 times more than what it costs consumers in Europe, Asia and North America. These high prices are often related to the high investment cost of fibre cables. Accordingly, the prices remain high in order to recoup the investments [24].

Historically, Sub-Saharan Africa has the highest broadband cost. Figure 2 shows that Sub-Saharan Africa (of which South Africa is a member) pays up to 810% of the monthly GNI (gross national income) per person for internet costs. The average cost for the world (calculation based on 150 participating countries) is 219% of the monthly GNI per person for internet costs. This fixed broadband basket was calculated by using the monthly subscription cost for an entry-level broadband package per country [5].

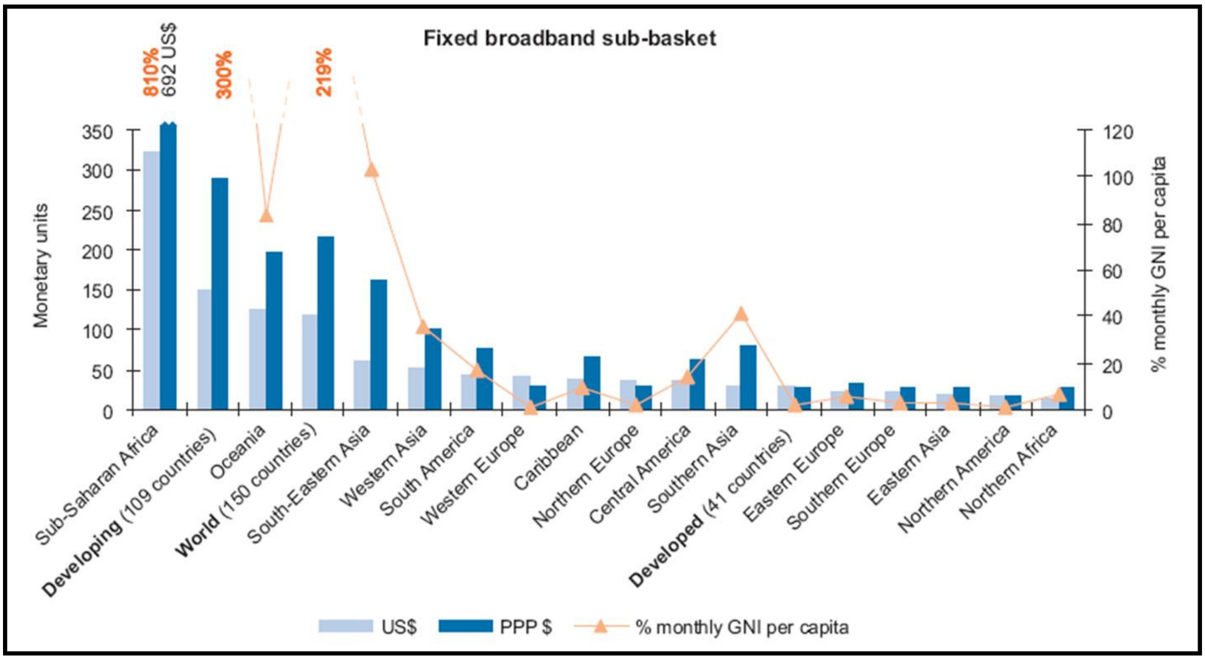


Figure 2: Cost of broadband internet access in countries of the world [5]

South Africa currently has a rather small internet population (compared to international figures) due to the historically high broadband prices, but this is all set to change. Should the cost of internet access be lowered, millions of new internet users may be connecting to the internet. Unfortunately, not all of these electronic devices will be properly prepared for the onslaught of Trojans, viruses, worms and hacks [6].

2.1.4 Trend 4: Shortage of IT education

The current restrictive bandwidth indirectly affects the availability of IT education in Africa. Since current internet connections are costly, it is mainly used by urban users that need it for their professions. The logistics of internet connections also make it difficult to reach the rural areas of Africa. As a result, IT education has not permeated throughout the African community, especially not to those areas with limited connectivity. *"The existence of this digital divide impedes the possibilities of improvement that such technologies can offer to the most underprivileged… More than 80% of the* *population of the planet is literally excluded from the global information networks that provide economic, cultural, political and social interactions…"* [14].

The shortage of IT education has a direct impact on the extent of usability of computers and IT within the everyday life. This may have a negative impact on strategic information security, since there is such a large gap between people effectively using IT and people rarely using IT to facilitate information security. It represents the inequality of possibility in relation to information access, knowledge and communication networks. In addition, many countries ship outdated PCs to Africa to help people there to increase IT education. However, this does not work as it requires them to run old and outdated software which makes them open for attacks [13].

Building on this digital divide, is the usability divide: technology is so complicated that many people cannot use a computer to its full capability, even if they got one for free. *"… Many others can use computers, but don't achieve the modern world's full benefits because most of the available services are too difficult for them to understand. Almost 40% of the population has lower literacy skills, and yet few websites follow the guidelines for writing for low-literacy users …"* [14]. In addition, IT education often is theoretical in nature, with little practical experience included to further understanding.

2.1.5 Trend 5: Absence of African languages

The absence of African languages in cyber space stands in direct relation to a shortage of IT education. It has a direct impact on the vulnerability of the African cyber space due to a lack of cognizance. Although many of the people staying in South African rural areas have acquired some computer skills, the basic computer use language is dominated by English [16]. Some scholars have considered the English language as a predictor of ICT adoption, given that the adoption and use of the internet may require English proficiency [2].

In many instances, computer users are willing to learn about cyber space, but are restricted to do this since African languages are used minimally in cyber space. For example, when the computer needs to be *switched off* (the process needs to END), the user needs to click on the *START* button. This is not an easy concept to grasp for people who are fluent in English, let alone someone who is not (see Figure 3).

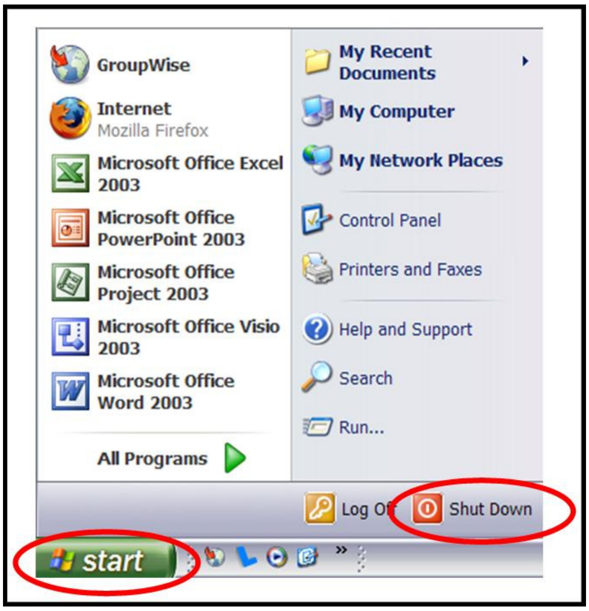


Figure 3: Windows shut down function

Many African computer users do not necessarily understand error messages or warnings about cyber fraud that are not presented in their mother tongue. As a result, the absence of African languages in cyber space poses a potentially serious threat to cyber space fraud and vulnerability to cyber space fraud. Google, however, has made some progress in this regard. Google South Africa has language options for English, Afrikaans, Sesotho, IsiZulu and IsiXhosa (see Figure 4). Although progress has been made, it is only a translation of the interface and not necessarily of the content.

2.2 Cyber threats

A cyber threat is a more immediate danger in the form of a declaration of an intention or a determination to inflict harm on another within the cyber domain.

2.2.1 Threat 1: Interfraud

Interfraud is any deception scheme that uses one or more online service to present deceitful solicitations to prospective victims, to conduct falsified transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme. Interfraud schemes can generally be divided into two groups: large number of victims for small per-victim losses, or small number of victims for large amounts of per-victim losses [25].

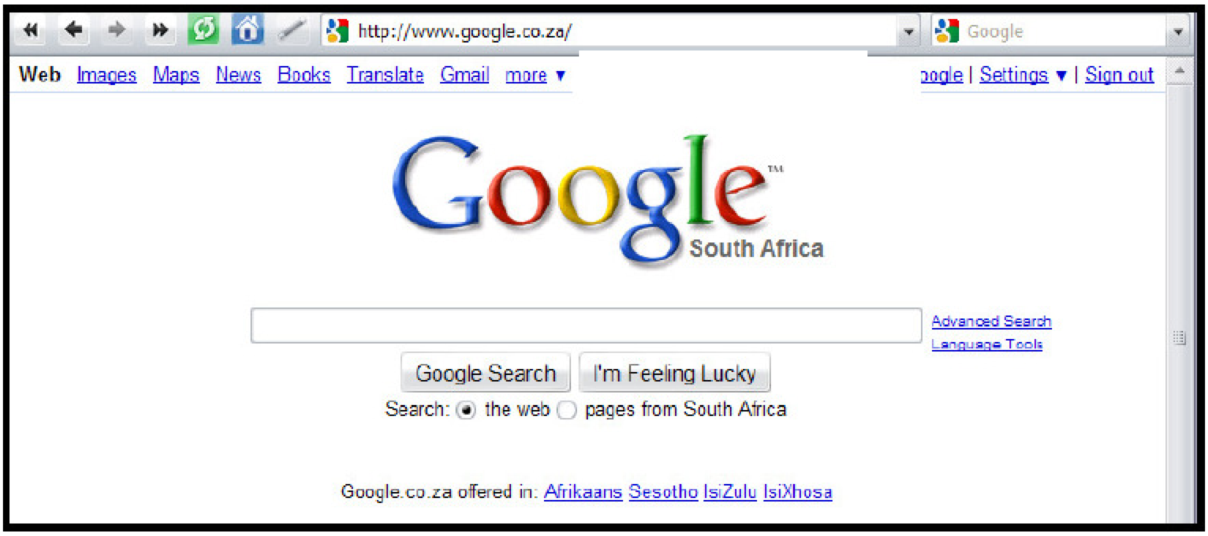

http://www.google.co.za/
Google
Web Images Maps News Books Translate Gmail more ▾
oogle | Settings ▾ | Sign out
Google
South Africa
Advanced Search
Language Tools
Google Search
I'm Feeling Lucky
Search: ● the web ○ pages from South Africa
Google.co.za offered in: Afrikaans Sesotho IsiZulu IsiXhosa

Figure 4: Google South Africa's language options

The cyber environment is rife with interfraud schemes, with a number of innovative variations on each possible scheme. Internet fraud can take place on computer programs such as chat rooms, e-mail, message boards or websites. Some examples include the advance fee scams (also known as the 419 scams, Nigerian scams or Spanish prisoner scams), purchase scams, dating scams, click fraud, money transfer scams, auction and retail scams. Interfraud is a very important aspect of the cyber impact and is crucial in the development of strategic information security. The FBI's 2009 list of the top ten cyber crime perpetrators features four African countries: Nigeria in the third place, Ghana in the sixth place, South Africa in the seventh place and Cameroon in ninth place [10].

2.2.2 Threat 2: Phishing

Where hackers and computer criminals originally attacked computer systems in an attempt to gain fame, their focus gradually started to shift from around 2003 to pursue fortune actively in a more sophisticated way [26]. The term *phishing* was coined in 1996 when thieves stole America Online (AOL) accounts using email as a proverbial fishing hook to steal passwords. Ph is a common hacker replacement for the letter f, and reminds of the older hacking type, phone *phreaking* (the act of gaining illegal access to resources of telecom networks, usually with the intention of making free long distance phone calls) [7].

Phishing is an attempt by a third party to solicit confidential information from an individual, group or organisation. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials and other sensitive information, which they may then use to commit fraudulent acts. These attacks are usually facilitated by mimicking specific, usually well-known brands and aims to elicit financial gain by employing social engineering and technical deception [3].

A number of different variations of phishing exist:

- **Man-in-the-middle (MITM) attacks -** a system attack during which a malicious individual can read, insert and modify information between the victim computer and the destination computer or website without their knowledge.
- **Third-party shortened URLs -** third-party organisations offers free services designed to provide shorter URLs.
- **Bad domain names -** purposeful registration and use of bad domain names, e.g. instead of registering *http://privatebanking.mybank.com,* the following *mybank.**privatebanking**.com* is registered.
- **Host name obfuscation -** URLs are presented as IP address, and not domain name, e.g. instead of *http://mybank.com: ebanking@evilsite.com/phishing/fakepage.htm,* the following *http://mybank.com:ebanking@210.134.161.35/login.htm* host name is used.
- **Smishing -** an attempt to get a mobile device owner to download a Trojan horse, virus or other malware by clicking on a link included in a SMS text message.

Phishing is an active threat within South Africa. The South African Banking Risk Information Centre (SABRIC) is regularly warning local banking clients to be careful with their banking credentials. SABRIC recently reported that the number of phishing scams targeting consumers are continuously increasing, and becoming more sophisticated [22].

2.2.3 Threat 3: Pharming

Pharming is a form of online fraud where pharmers rely on falsified websites and theft of confidential information to perpetrate online scams. The pharming attack misdirects internet users of trusted brands to false storefronts set up specifically to harvest identities. The crime is typically accomplished through cache poisoning of domain name servers (DNS) or domain hijacking, in which registrars are tricked into moving domains [19]. The term *pharming* is chosen because the attackers plant a single poisoned seed (incorrect IP address) in the DNS and as a result poisons the entire crop feeding from that one seed. Again, the f in farming is replaced with the common hacker replacement ph.

Unlike phishing (refer to Threat 2), pharmers work invisibly and do not rely on spam to lure victims to their fraudulent websites. Pharming is a form of domain spoofing, where pharmers change a local DNS to redirect the victim's web request to a fake website - pharming attacks direct victims to a fake website even if they typed the correct address of the intended website into their browser. If the pharmers designed the fake website to look like the legitimate website, the victim has no way of knowing it is a fraudulent website [4]. Figure 5 shows a legitimate website, and Figure 6 a fake website. The only difference between these two websites, reckoned on face value, is the difference in URL.

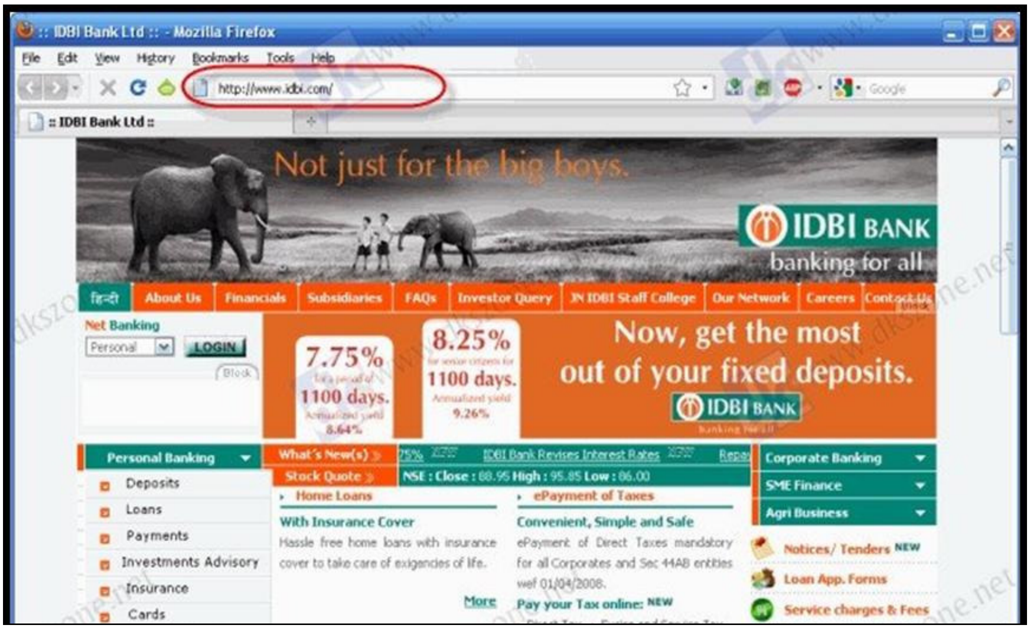
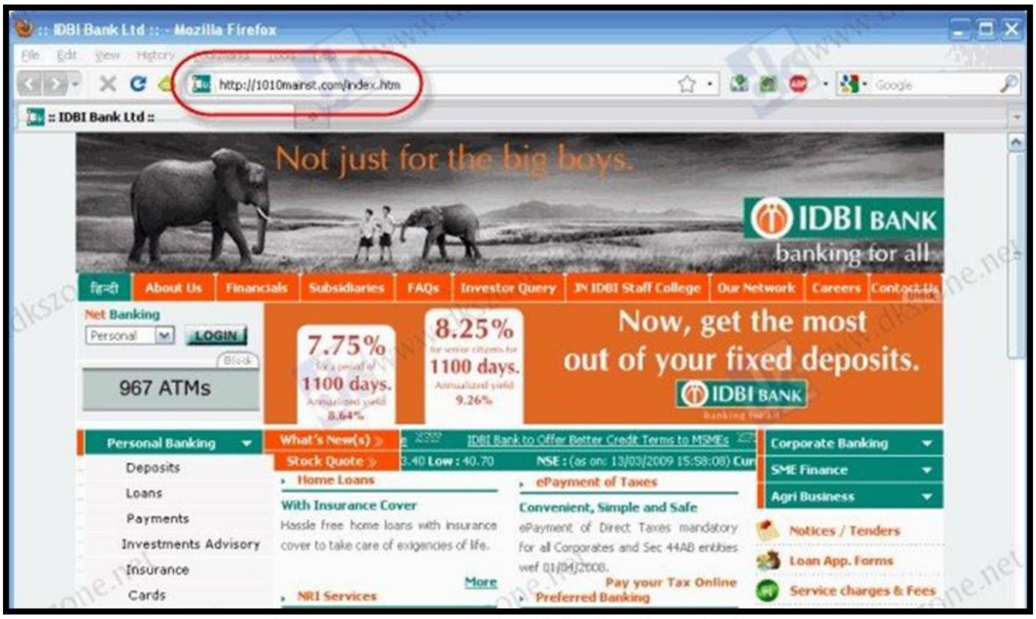


Figure 5: Genuine IDBI Bank website



Not just for the big boys.

Now, get the most out of your fixed deposits.

IDBI Bank to Offer Better Credit Terms to MSMEs

3.40 Low : 40.70 NSE : (as on: 13/03/2009 15:58:08) Cur

With Insurance Cover

Hassle free home loans with insurance cover to take care of exigencies of life.

Convenient, Simple and Safe

ePayment of Direct Taxes mandatory for all Corporates and Sec 44AB entities wef 01/04/2008.

Pay your Tax Online

Figure 6: Fake IDBI Bank website

2.2.4 Threat 4: Malicious attacks

Africa is home to about 100 million PCs, 80% of which are estimated to be infected with some kind of malware. This malware infestation is partly due to the intense poverty throughout the continent directly contributing to the pervasive distribution of pirated software and the inability to pay for anti-virus protection. Although the high percentage of malware infected computers is a dire problem, the current situation is that most internet access occurs via dialup. With the increased broadband access planned for 2011, these unprotected computers will become an easy target for bot herders [9].

"… While western countries have partially learned to neutralise the threat of computer viruses, Africa has become a hive of trojans, worms and exploiters of all stripes. As PC use on the continent has spread in the past decade (in Ethiopia it has gone from 0.01% of the Ethiopian population to 0.45% through 1999-2008), viruses have hitched a ride, wreaking havoc on development efforts, government programmes and fledgling businesses" [13]. Any kind of malicious attack, as part of failing information security, shows the impact of the cyber world on the every day world.

2.2.5 Threat 5: Social networking

Social networking is a network service that focuses on building and reflecting social networks or social relations among groups and individuals. Although it has numerous benefits and opens several opportunities for global communication, it poses an active threat of publicly disclosed breaches and compromises. Not only is there specific malware designed to target these sites exclusively, but social networking enables cyber stalkers to get unlimited information on any target. This is also an ideal breeding ground for identity theft, were most anything can be found on the internet if you know where to look and have enough patience.

People also often forget that they are on a public global domain. Especially with day-to-day human computer interaction, people tend to forget that it is not just a document being typed on a faceless computer, but rather text that is posted on a public forum, to be read by anyone that has the time and understands the language. The topic of potential personal security breach received a wide public audience when the then new head of the Secret Intelligence Service (MI6) was left exposed after his wife published intimate photographs, family details and geographical information on her Facebook profile. His wife did not enable the optional privacy protection offered by the social network, making their home and work addresses visible to any of the site's 200 million users in the open-access London network [12].

The next section uses the knowledge gained through understanding the relevant cyber trends and threats to prepare a proactive forensic readiness plan to aid in the strategic information security plan.

3. A proactive approach to information security

Due to the digital nature of many modern day business transactions, it is necessary to ensure digital forensic readiness as part of the information security strategy. This can relate to word processing documents, spreadsheets, emails and websites. Accordingly, digital evidence is any information that can be secured from an information system and used during the course of a civil or criminal legal procedure.

In general, digital forensics relates to the production of legal evidence found within information contained in computers and storage media. Digital forensics mostly takes the form of a reactive approach. Forensic readiness, on the other hand, refers to the achievement of an appropriate level of capability by an organisation to be able to collect, preserve, protect and analyse digital evidence so that this evidence can be used effectively in any legal or disciplinary matters. Forensic readiness mostly takes the form of a proactive approach. Forensic readiness has much in common with business continuity, contingency planning and capability building.

Due to problems associated with the acquisition of digital evidence, it is necessary to take proactive measures to ensure the admissibility of digital evidence. Thus, especially in the wake of a cyber trend or threat, an ideal forensic readiness will demonstrate the following characteristics [15] [20]:

- management function that identifies and establishes the required relationships necessary to support investigations,
- compliance with applicable laws relevant to the jurisdiction,
- effective management for the processing of disclosure required for legal, data protection and freedom of information purposes,
- established point of contact with law enforcement,
- trained first responders that can secure information security assets at the scene of an investigation and may appear as witnesses in legal proceedings,
- effective electronic records management that is capable of producing digital evidence,
- diagnostic indicators for all identified scenarios and that would call for the plan to be put into effect,
- details of the likely sources of digital evidence (internal and external to the organisation) that can support the investigation,
- description of the processes and procedures to be followed during the investigation,
- description of the desired outcomes of the investigation and the expected deliverables, and
- forensic readiness planning function aligned with the business continuity function.

By designing and implementing a comprehensive security strategy to identify and manage internal interdependencies unique to the organisation, it is possible to take a proactive approach to information security. Table 1 shows the mapping of the information presented in this article to the original definition of strategic information posed in Section 1.

Table1: A proactive approach to strategic information security

Proactive action	Strategic information security definition
Understand the trends and threats	Identify
Understand the cyber environment	
Implement Corporate Governance	mitigate/manage
Initiate forensic readiness measures	
Understand the market conditions	Develop
Identify drivers that pose risks	threatens resilience
Identify drivers that pose opportunities	continued survival
Build a culture of constant awareness	early stage

Within the context of Table 1, cyber trends and threats may look like only a small aspect, but due to the dynamic nature of the cyber domain, it is very important. As a result, a lot of attention has been given to some identified cyber trends and threats in Section 2. Thus, by understanding the trends, threats and general cyber environment, implementing Corporate Governance (as part of the information security strategy), initiating forensic readiness measures, understanding the market conditions, identifying drivers that pose both risks and opportunities, and building a culture of constant awareness, it is possible to use the impact the cyber world has to ensure information security. These activities map directly on the definition of strategic information security and provide a more secure environment in which organisations can proactively act to prevent or minimise the effect that cyber attacks and malicious intrusions might have on the organisation.

4. Conclusion

This article introduced the impact of the cyber reality by addressing current cyber trends and threats in Africa. It proposed forensic readiness as proactive measure to ensure strategic information security, and presented a mapping of the cyber impact and forensic readiness actions on the definition of strategic information security. The understanding of the cyber impact and the proactive actions that organisations can take to address strategic information security may lead to a decrease in global vulnerabilities. Thus, by facing the impact that the cyber world may have on the information strategy, it becomes possible to work towards global international information security.

References

[1] Anonymous,"Internet penetration", Accessed 201006/14, Available online at http://upload.wikimedia.org/wikipedia/commons/a/af/Internet_Penetration.png.

[2] M. Billon, R. Marco and F. Lera-Lopez, "Disparities in ICT adoption: A multidimensional approach to study the cross-country digital divide", *Telecommunications Policy,* vol. 33, pp. 596-610, 12 2009.

[3] P. Cassidy, "Phishing activity trends report - 4th quarter 2009", Accessed 201006/14, Available online at http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf.

[4] Consumer Fraud Reporting, "Pharming - fake websites, real IP addresses - stealing your personal financial information ", Accessed 201006/10, Available online at http://www.consumerfraudreporting.org/pharming.php.

[5] RL Cottrell and U. Kalim, "New E. Coast of Africa fibre", Accessed 200911/19, Available online at https://confluence.slac.stanford.edu/display/IEPM/New+E.+Coast+of+Africa+Fibre.

[6] K. Doyle, "Could SA lead cyber crime rankings?", Accessed 201006/14, Available online at http://www.itweb.co.za/index.php?option=com_content&view=article&id=27948:could-sa-lead-cyber-crime-rankings.

[7] Global Oneness, "Phishing - History of phishing", Global Oneness, Accessed 200912/10, Available online at http://www.experiencefestival.com/a/Phishing_-_History_of_ phishing/id/1845385.

[8] R. Halbheer, "The Africa cable - A chance for Africa! - A threat for the internet?", InformationSecurity.com, Accessed 200910/10, Available online at http://www.infosecurity-us.com/blog/2009/10/7/the-africa-cable--a-chance -for-africa--a-threat-for-the-internet/28.aspx%20-.

[9] Intellibriefs, "Africa – home of the world's largest cyber pandemic", Accessed 200908/10, Available online at http://intellibriefs.blogspot.com/2009/10/africa-home-of-worlds-largest-cyber.html.

[10] Internet Crime Complaint Center, "2009 Internet crime report," IC3, pp. 1-26, 2009.

[11] Internet World Stats, "Internet usage statistics - The internet big picture: World internet users and population stats", Accessed 201006/08, Available online at http://www.internetworldstats.com/stats.htm.

[12] J. Lewis, "MI6 chief blows his cover as wife's Facebook account reveals family holidays, showbiz friends and links to David Irving", Accessed 201006/14, Available online at http://www.dailymail.co.uk/news/article-1197562/MI6-chief-blows-cover-wifes-Facebook-account-reveals-family-holidays-showbiz-friends-links-David-Irving.html.

[13] C. Michael, "Computer viruses slow African expansion", Accessed 200910/05, Available online at http://www.guardian.co.uk/technology/2009/aug/12/ethiopia-computer-virus.

[14] M. Milicevic, "Cyberspace and globalization", Accessed 201006/14, Available online at http://www.ais.up.ac.za/digi/docs/milicevic_paper.pdf.

[15] JJ Murphy, "Forensic readiness", Dexisive, Accessed 201003/06, Available online at http://www.dexisive.com/docs/Forensic%20Readiness.pdf.

[16] B. Musinguzi, "African languages absent in cyber space", Accessed 201006/08, Available online at http://allafrica.com/stories/200804081119.html.

[17] Nortel Networks, "Integrated security – a proactive, cross-functional approach for using security to enhance competitiveness of the enterprise, White paper", Accessed 201004/08, Available online at http://www.nortel.com/solutions/security/collateral/nn109100.pdf.

[18] J. Otieno, "Low internet usage the bane of Africa's digital media", Accessed 201004/08, Available online at http://allafrica.com/stories/201003190904.html.

[19] D. Radcliff, "How to prevent pharming", Accessed 200912/10, Available online at http://howto.techworld.com/ networking/1615/how-to--prevent-pharming/.

[20] R. Rowlingson, "An introduction to forensic readiness planning," QinetiQ, Tech. Rep. NISCC Technical Note 01/2005, pp. 1-14, 2005.

[21] D. Smith, "Five million now online as web access grows in South Africa", Accessed 201004/08, Available online at http://www.guardian.co.uk/world/2010/jan/14/internet-five-million-south-africa.

[22] SPAMfighter News, "SABRIC - Phishing scams rising in South Africa", SPAMfighter News, Accessed 201007/07, Available online at http://www.spamfighter.com/News-14693-SABRIC-Phishing-Scams-Rising-in-South-Africa.htm.

[23] Symantec, "State of Enterprise Security 2010," Symantec Corporation, pp. 1-16, 2010.

[24] A. Twinomugisha, "Why are African internet access prices still high?" Africa Business Source, vol. Experts, 2010/04/01. 2010.

[25] US Department of Justice, "Mass-marketing fraud", Accessed 201004/12, Available online at http://www.justice.gov/criminal/fraud/internet/.

[26] Websense, "Phishing and pharming," Websense, pp. 1-10, 2005.